

RED ALERT

Red Alert is an attempt to map the global fight against money laundering; a kind of travel guide through the teeming jungle of crimes, risks, regions, countries, criminals, terrorists, cases, banking products and services, laws and standards and money laundering programme design across the world.

In this book the following are comprehensively examined.

In Part 1 - Crime Related Materials:

- All predicate offences to money laundering
- Businesses and professions posing an increased risk of money laundering
- Regions and countries posing increased money laundering risks, and country risk methodologies and sources
- Major lines of banking businesses, including retail and commercial, cards, correspondent and private banking, brokerage, investment banking and asset management, as well as particular money laundering risks and potential vulnerabilities
- Major money laundering related laws, regulations and standards

In Part 2 Crime Related Cases, with more than 500 case examples and profiles:

- 250+ profiles of the most dangerous and deadly organised criminal gangs and terrorist groups, including details of the most reprehensible terrorist attacks
- 150+ criminal case profiles including landmark corruption, fraud, market abuse and drug trafficking, organised crime and terrorist financing cases
- 100+ Enforcement cases against financial institutions

...and much more.

"Amazing amount of information"

Lord James Sassoon, Former FATF President 2007/8

"Impressive...a wealth of information"

Boudewijn Verhelst, Chair Egmont Group until 2013

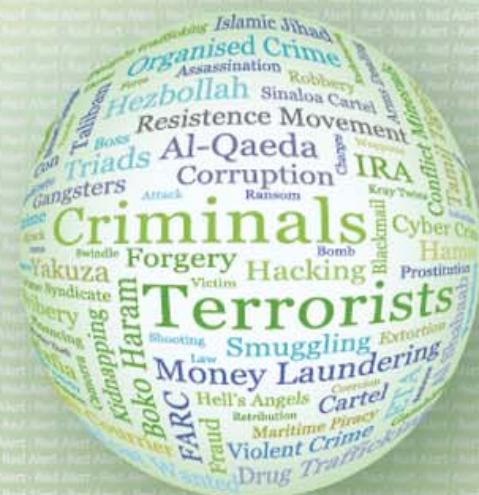
"The ultimate guide to ML detection and prevention"

John Mair, EBRD

Cusack

**RED ALERT: Money Laundering Cases and Materials
for Money Laundering Prevention Professionals**

RED ALERT



**Money Laundering Cases and Materials
for Money Laundering Prevention Professionals**

2014 - Issue I

By John Cusack

Red Alert

Author's Note

Dear Reader,

I like to think of "Red Alert" as a personal travel guide through the teeming jungle of crimes, risks, regions, countries, criminals, terrorists, cases, banking products and services, laws and standards and programme design relating to the World of Money Laundering Prevention.

As a money laundering professional you are faced with an increasingly difficult set of tasks and an environment that is complex and dynamic. As such learning holds the key to success and will provide its own rewards. As Benjamin Franklin once said, "For the best return on your money, pour your purse into your head."

I hope you will find this both of interest and of use, in placing your work in a broader context and in navigating through the challenges of your own role and in refining the nature of your contribution.

As you read the Book, either from start to finish or by focussing first on particular areas of interest, consider the words of Confucius, "Learning without thought is labour lost; thought without learning is perilous."

The Book is right up to date to the end of 2013. At the end of the Book I have included important developments to the end of March 2014.



John Cusack - March 2014

About the Author



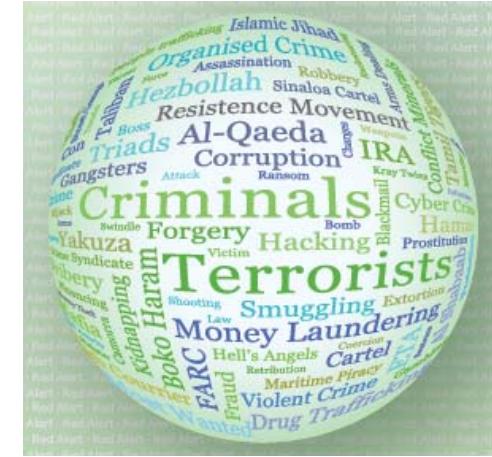
John Cusack is one of the World's longest serving Money Laundering Prevention Heads, joining UBS over 20 years ago, as a qualified English Lawyer, undertaking senior roles in both Legal and Compliance across much of the firm, including in Investment Banking, Correspondent and Commercial Banking and Retail Banking and

Wealth Management. He led UBS in its efforts in managing and mitigating money laundering risks as its first Global Head of Money Laundering Prevention, Sanctions Compliance and Anti Bribery and Corruption by both designing appropriate programmes and ensuring operational effectiveness.

John Cusack has recently agreed to take up a similar position at Standard Chartered Bank PLC as Global Financial Crime Head which will commence later in 2014.

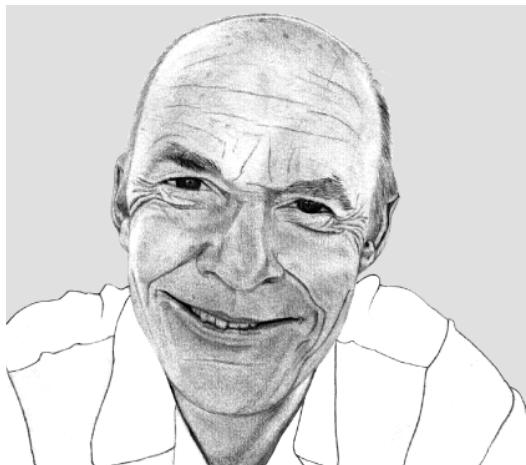
John Cusack has acted as a Chairman and has been a constant member of the industry leading Wolfsberg Group of International Banks for more than 10 years and has led and contributed to numerous Wolfsberg initiatives. He has regularly provided advice to law and policy makers, law enforcement agencies and colleagues in the private sector.

Red Alert



**Money Laundering Cases and Materials
for Money Laundering Prevention Professionals
2014 Edition - Issue 1**

By John Cusack



This book is dedicated to the hard work of all those involved in money laundering prevention and in particular to one of its brightest sons, and so to the memory of
MATTHEW COOPER

On 29 March 2011 we lost Matthew Cooper, known to many in the world of money laundering prevention as one of its most dedicated students and gifted teachers. To quote from the website established in memory to Matt, “the AML community lost one of its most knowledgeable and colourful members, someone who was universally liked and respected, a rare feat in our business.”

Matt had worked in both public (for the UK government in many roles, including fraud prevention at the sharp end and in the civil service at the smart end) and with the private sector with Barclays as Group AML Head and as deputy Global AML Head at UBS and then latterly at AMEX. Matt had also been one of the most influential and dedicated contributors to the Wolfsberg Group as well as with other industry bodies championing and always working together to find common solutions and practical ways to move things forward. In all of these roles, Matt was infectious and passionate about his work but also had time for colleagues and would listen and provide experienced and wise counsel whenever it was needed or whenever it was sought.

To many Matt will always be a friend; one sorely missed but whose lasting contributions reminds of his gifts and his unique talents. This book was inspired together with Matt Cooper and it is also for this reason that I dedicate this book to his memory.

Red Alert

Money Laundering Cases & Materials

Contents

Part 1

Introduction, 1
Contents, 3
Five Recommendations to “Effectively” combat Money Laundering, 5-10

Facts & Figures, 11-12
What is Money Laundering?, 13-18

Section 1 - Money Laundering Crimes, 20-126
Section 2 - Money Laundering Risks, 128-222
Section 3 - Money Laundering Laws & Regulations, 224-279
Section 4 - Money Laundering Prevention Programmes, 282-314

Part 2

Introduction, 2
Contents, 4

Section 5 - Regions, Countries, Criminals & Terrorists, 318-506
Section 6 - Terrorist Attacks, 508-537
Section 7 - Criminals/Cases, 540-668
Section 8 - Enforcement Cases, 670-738

Breaking News, 739-743
Notes, 745-812
Abbreviations, 813
Index, 814-844
Reviews of this Book, 845-847

Acknowledgements

Much of the information that forms the basis for the content of this Book comes from the public domain. The sheer amount of information that is publicly available is staggering but for professionals on the front line, their ability to locate, read, digest and consider the importance or otherwise of much if this information is severely limited. I have unashamedly relied on information and publications from the FATF, the World Bank, the UN, the IMF and the OECD as well as many other international, regional, national and local bodies, both public and private, that have reputations for both integrity and accuracy. I have also relied on information from the world wide web, in particular from Wikipedia and other sources where I feel this is useful and informative.

I then take a large step back and tell it as I see it. I have used a mosaic analysis, undertaken by some securities research professionals, building up from many sources as complete a picture as I can about our targeted subject, and in so doing providing greater insight. This is attempted but how this information is presented and how this is reshaped to provide the reader with an interesting read is the product of the many experts and contributors from UBS and elsewhere but ultimately the responsibility of the Author. As such, nothing in this book should be attributed to UBS and UBS does not guarantee the accuracy of the data nor necessarily agree with any of the contents or contributions.

Whilst I have tried to author a great deal of this book, the subject and the task is too great for any one person. I have relied upon an original concept discussed with my dear friend and departed colleague, Matt Cooper, and from the many experts and professionals at UBS. In particular all my senior AML team, including Jonathan Shih, my successor and Global Head of AML, Elaine Banar, Matt Chapman, Patricia Sullivan, Mike Bixon, Jean Marc Futterknecht, Elodie Chalmers, Tara Loftus, Pierre Grumbacher, Rainer Hoerning and Kevin Daynes. I would also like to thank the following UBS AML Team members for their valuable contributions including, Andrew Clayton, Florian Michel, Chris McNeil and Erik Zorteia from the Asian Team, Ulrich Ehrlsam, Martin Rimann and Corinne Marbacher from the Swiss team, Dominic Elsby, Mark Nelson, Dan Riddle and Netsanet Solomon from the UK team and Robert Berg and Priti Singh from the Americas team. I would also like to thank Jonathan Bibby, Steve Livermore and Anu Sharma from UBS Compliance for their contributions. I also appreciate contributions from former UBS experts, Joe Scavo, Sheryl Cottrell, Sam Rahman, Abnash Sagoo and Mark Starbuck. Special mention goes to the AML Compliance Education & Training team, including Derik Riesche and Christina Aur and an extra special thank you to Ramona Strelbel, Tom Duckmantion, Jigna Rathod, Hanna Patel, Shamayim Watson and Frances Cusack. I would also like to thank all those people who agreed to be interviewed or who have provided their opinions on certain aspects covered by this Book. I have been very fortunate to be able to benefit from the deep knowledge of many across the money laundering prevention profession, from private sector specialists, to law and policymakers, regulators, investigators and NGOs.

I would also like to thank Bernadette Jacobs, Victoria Meyer and Krina Patel for their administrative production and design and illustrative abilities respectively without which this book could not have been created or published and I would also like to express my appreciation to Andrew Williams, former UBS Global Head of Compliance and Markus Diethelm, UBS General Counsel for their continuous and wholehearted support for the AML Programme and team at UBS and the work that we do. I would also like to thank Hans-Peter Bauer and Neil Stocks for both their intelligence and integrity and from whom I have learned and been privileged to benefit from their advice and opinions over most of my professional career.

I also acknowledge the reader, those of you with the spirit of enquiry, the knowledge and the dedication and the tenacity to work and take an interest in money laundering prevention. Your tasks are important, difficult sometimes dangerous and mostly underappreciated, but not by your peers and colleagues and not by those that understand truly what you do. If you agree, disagree, wish to add or comment on any aspect of the contents of this book you are encouraged and welcome to do so.

Finally I would also like to thank my parents Brian & Anne Cusack for their constant support and to my children, Tomas & Hannah Cusack, for their patience as I worked on the book, and for being themselves today, tomorrow and always.

You can contact me at John-Paul.Cusack@ubs.com/jpcusack78@gmail.com or at www.redalert.org.uk.

All rights reserved without limiting the rights under copyright, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written permission of the author of this book.

Whilst every care has been taken to ensure the accuracy of the content of this work, no responsibility for loss occasioned to any person acting or refraining from action as a result of the material in this publication can be accepted by the author.

Where opinion is expressed it is that of the Author and does not necessarily coincide with the views of UBS or anyone else.

This Book is published to encourage discussion and comment and so whilst the material in this publication is copyrighted, the Author encourages the use of this work and so permission to the limited photocopying of items for internal or personal use will be normally granted. To reprint individual sections or sub-sections please e-mail your request to the Author.

Cover image and similar world cloud images by Victoria Meyer.

First Published 2014 (March)
Copyright 2014 John P Cusack

Introduction

This Book is intended to serve as a comprehensive source of information for money laundering professionals that wish to better understand, establish or improve their money laundering, terrorist financing, fraud, sanctions, bribery and corruption prevention frameworks (hereafter referred to as money laundering). These issues are of utmost importance and increasingly so, as the international community is relying on money laundering professionals to assist in successfully preventing, detecting and reporting money laundering in order to fight the devastating economic and social consequences of these criminal activities.

No Financial Institution worthy of its license, and mindful of its reputation and the risks, both criminal and civil that exist will deal knowingly with the proceeds of crime. More than that a financial institution will want to assist government authorities in every way in disrupting criminal funds, interdicting criminal flows and gathering intelligence to follow criminal trails. In addition to following the requirements by anti money laundering standard setters, as presented for compliance by applicable laws and regulations, Financial Institutions are faced with the challenge of designing appropriate AML Programmes which respond not only to the law, but should be based on the financial institutions own business activities but also reflect the changing threats posed by criminals and terrorists, to societies priorities championed by various stakeholders and to the pace of change within the Financial Services Industry.

This challenge is not all straightforward and requires a profound understanding of criminal behavior, the actors themselves, their criminal activities and in particular their attitudes and methods used in carrying out their crimes and laundering the proceeds of these crimes. In this criminals have a serious information advantage. As Sun Tzu wrote in the Art of War, "If you know the enemy and yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."¹

The Book is intended to reduce the criminals advantage, to alter the current imbalance and to get to know the criminal and his ways better. They provide money laundering prevention professionals, those that design, implement and test and for those that are also interested in combatting money laundering on a day to day basis with a comprehensive basis to improve both their understanding and ultimately improve effectiveness.

This Book is divided into **2 Parts** each divided into **4 Sections**, with, **5 Recommendations to "Effectively" combat Money Laundering; Money Laundering Facts and Figures; and What is Money Laundering?** providing an introduction to Part 1.

Part 1

Section 1 starts by looking at each of the **predicate offences to money laundering**, recognising that whilst the motive for economic crime, for money, may be similar there are many differences that set each of these crimes apart and make them attractive to criminals. For each, a look back through time provides the context in which to place criminal activities and relevant statistics aim to show the scale and size of the profits earned by the criminals, why criminals find these crimes so attractive and how criminals launder their money.

Section 2 focuses on **money laundering risks**, those that a money laundering prevention professional should be most concerned about and is divided into 4 Sub-sections.

Sub-section 1 contains specific information from **FATF, the US and the EU and then from the Wolfsberg Group** and other sources focussing on the main areas of inherent money laundering risk, customers, products and services and the risk of distribution or channel risk, geography and country risks.

Sub-section 2 focuses in more detail on the main **Customer** types that pose increased risks.

Sub-section 3 analyses in more detail the core **Products and Services** via the main business operations conducted by Financial Institutions. For each of these major lines of business, the most important risks are identified alongside distribution or channel risks as well where appropriate alongside key scenarios identified that may pose the greatest risks and may need to be addressed.

Sub-section 4 deals with **Geography or Country Risk**, looking at methodologies, examples and many of the most important sources, in order to identify relative risk classifications between Countries. Country Profiles themselves particularly countries that are significantly vulnerable and/or exposed to money laundering and/or where terrorist groups or organised criminal gangs operate or call home are included in Part 2, Section 5 (see later).

Section 3 provides a comprehensive guide to the **most important legal instruments**, the international conven-

tions and treaties that formulate the necessary political agreements and indicate political will to fighting serious crime and on the proceeds of and financial facilitation of crime. This is supplemented by an overview of work conducted over the years by the Financial Action Task Force (FATF) and similarly of that of the leading industry body the Wolfsberg Group, focusing on a chronology of its publications and contributions. Finally a more detailed examination of existing Sanctions and Embargo laws and regulations completes this Section 3.

Section 4 offers suggestions on how to manage and mitigate money laundering risks, with details about **Risk Assessment and AML Programme** design and frameworks for each of money laundering, sanctions compliance, anti-bribery and corruption, and anti-fraud Programmes.

Part 2

Section 5 provides an insight into more than **250** of the most powerful **criminal gangs** and the most dangerous **terrorist groups** operating still today and some of histories most notorious, are profiled. In doing so, it demonstrates the continued prevalence of these groups their menace and it also demonstrates that few areas of the world have escaped the insidious attentions of these parasitical and determined criminal organisations. All **Regions** of the world are included, focussing on some **Key Countries** in these regions, with increased risks and where these organised criminal gangs and or terrorists call home. The gangs and groups include mafia type organisations, street gangs, prison gangs and other gangs that are involved in substantial collective criminality and terrorist organisations, religious, political and ethnic.

Section 6 continues with a focus on Terrorists with a chronology and short summary of the **Worlds Worst Terrorist attacks** over the last 100 Years by the number of fatalities which is also followed by the **Worlds Worst Terrorist Attacks on Airlines** amounting to up to more than **150** major incidents.

Section 7 continues the focus on serious crime, the financial rewards and the laundering of the proceeds of crime by looking at more than **150** of the most renowned **Criminal Cases**, covering all manner of crimes, including corruption, drug trafficking, fraud, insider dealing and market manipulation and robbery, and many more. Whilst these cases can be seen as often exceptional, they nevertheless have to a large extent driven the legislative and public policy agenda in response to the concerns raised once these cases have come to public attention.

Section 8 completes the case theme, this time focussing

on more than **75** Financial Institution **Enforcement Cases**. FIs have been publicly sanctioned and/or fined for money laundering and or sanctions compliance related failings and these are summarised in order to illuminate the pitfalls and the increasing expectations placed on financial institutions.

Final Remarks

The contents of this Book are a work in progress as it has not been possible to include everything of interest and because new revelations will bring to light new areas of concern new areas of vulnerabilities and new areas to focus on. For now it is essential that the current areas of concern highlighted in this Book are considered and where appropriate addressed by all those keen on managing and mitigating money laundering risks.

Note to Reader

Where text is underlined it indicates a more detailed summary or profile can be found in this book, usually identifying a major risk category, instrument of law, an organised criminal gang, terrorist organisation, attack, criminal case or enforcement case.

Further Information

For more information go to www.redalert.org.uk.

Red Alert Test

For readers interested in assessing their financial crime knowledge and testing themselves against the contents of this Book, a multiple choice test is available with approximately 250 tailored questions in aggregate but individual tests covering a number of themes; including: Bribery & Corruption; Organised Crime/Drug Trafficking; Other Crimes; Terrorism Finance; WMD Proliferation Finance; Fraud; Market Abuse; Sanctions; Customer Risks; Products & Services Risks; and Money Laundering Prevention Programmes. For details about how to take the test and receive a Red Alert Certificate of Achievement for one or more modules or for the entire Test, contact the author directly on jpcusack78@gmail.com.

Note on support to the National Autistic Society

From any profits generated from the commercial sale of this Book, a contribution will be made to The National Autistic Society (www.autism.org.uk)



Red Alert Money Laundering Cases & Materials

Contents - Part 1

Introduction

Five Recommendations to "Effectively" combat Money Laundering, 5-10

Facts & Figures 11-12

What is Money Laundering?, 13-18

Section 1 - Money Laundering Crimes, 20

- Introduction, 21

- Bribery & Corruption, 23

- Counterfeiting & Piracy of Products, 29

- Drug Trafficking, 35

- Environmental Crime, 42

- Extortion, 48

- Forgery, 50

- Fraud incl Tax Fraud & Cybercrime, 52

- Human Trafficking, 63

- Illicit Arms Trafficking, 66

- Insider Dealing, 69

- Kidnap, Illegal Restraint & Hostage Taking, 78

- Market Manipulation, 82

- Murder and Grievous Bodily Injury, 89

- Organised Crime, 93

- Smuggling, 100

- Terrorism Finance, 106

- Theft, Robbery & Trafficking, 118

- WMD Proliferation Finance, 123

Section 2 - Money Laundering Risks, 128

Sub-section 1 - Money Laundering Risks, 130

Money Laundering Risks Identified, 131

- Financial Action Task Force, 131

- United States, 133

- European Union, 134

- Other Countries, 134

- The Wolfsberg Group, 134

- Additional Sources, 135

Sub-section 2 - Customer Risks, 138

- Arms Dealers, 139

- Banks & Other Financial Institutions, 141

- Cash-Intensive Businesses, 143

- Casinos including Internet Gambling, 145

- Charities & Not For Profit Organisations, 152

- Gatekeepers, 154

- High Value Goods Dealers, 157

- Intermediaries, 161

- Money Services Businesses, 162

- Politically Exposed Persons, 166

- Precious Metals & Stones Dealers, 169

- Private Military Firms, 173

- Real Estate Agents, 175

Sub-section 3 - Products & Services (incl Channels) Risks, 178

- A Brief History of Banking, 179

- Asset Management, 181

- Brokerage / Securities, 183

- Commercial Banking, 186

- Correspondent Banking, 191

- Credit & Other Cards, 198

- Investment Banking, 201

- Retail Banking, 205

- Wealth Management / Private Banking, 209

Sub-section 4 - Country Risks, 214

- Country Risk Methodology & Sources, 215

- Financial Action Task Force / FATF, 215

- Sanctioned Countries, 216

- Wolfsberg Group, 217

- Basel Institute of Governance, 218

- Additional Country Sources, 218

- Hot Spots (in-Country and Regional), 221

- Diversion Risk or Close Proximity Risk, 221

- Free Trade Zones, 222

- Time Zone Risk, 222

Section 3 - Money Laundering Laws & Regulations, 224

- Introduction, 225

- AML Treaties, Conventions & Major Laws, 226

- FATF Recommendations and Work, 245

- Wolfsberg Group AML Standards & Work, 259

- Sanctions & Embargoes, 264

Section 4 - Money Laundering Prevention Programmes, 282

- Risk Based Approach, 283

- Risk Assessment, 285

- AML Programme, 295

- Sanctions Programme, 301

- Anti Bribery & Corruption Programme, 306

- Anti-Fraud Programme, 310

Contents - Part 2

Section 5 - Regions, Countries, Criminals and Terrorists, 318

Introduction, 319

Africa, 321

- North Africa, 322

- West Africa, 326

- The Horn of Africa, 330

- Eastern Africa, 332

- Central Africa, 337

- Southern Africa, 341

Middle East, 347

Asia, 370

- Southern Asia, 370

- South East Asia, 397

- Eastern Asia, 404

- Central Asia, 414

Oceania, 417

- Australia/New Zealand, 417/418

- Pacific Islands, 418

Americas, 419

- United States, 420

- Canada, 432

- Mexico, 435

- Caribbean, 443

- Central America, 446

- South America, 451

Europe, 469

- Eastern Europe, 470

- Western Europe, 485

Section 7 - Criminal/Cases, 540

Introduction, 542

- Corruption,

- Individuals/PEPs, 543

- Corporates, 561

- Environmental Crime, 568

- Fraudsters, 569

- Accounting Fraudsters, 569

- Advanced Fee Fraudsters, 581

- Hedge Fund/Investment Co Fraudsters, 582

- Ponzi - Pyramid Schemes, 586

- Rogue Traders, 588

- Private Banker Fraudsters, 606

- Tax Fraudsters - Tax Evaders, 607

- Others, 610

- Insider Traders, 611

- Kidnappers/Robbers/Extortioners/Forgers, 625

- Market Abusers, 629

- Traffickers, 642

- Illicit Arms Traffickers, 642

- Drug Traffickers (Organised Crime, 649)

- Goods Traffickers, 655

- Human Traffickers, 656

- Terrorism Financiers, 658

- WMD Proliferation Financiers/Sanctions, 664

Section 8 - Enforcement Cases, 670

Introduction, 671

- Chronology of FI Major Enforcement Cases over the last 25 years, 673

- Enforcement Cases, 675

Outlook Cases/2014 and beyond, 738

Breaking News, 739

Notes, 745

Abbreviations, 813

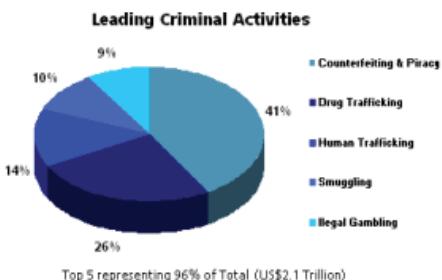
Index, 814

Reviews of this Book, 845

Five Recommendations to "Effectively" combat Money Laundering

Fighting crime has always been tough, increasingly so in a globalised world. In spite of law enforcement efforts, the age-old maxim “crime doesn’t pay” seemingly no longer applies as money laundering¹ continues to hit the headlines and ever greater estimates of criminal proceeds are announced.

According to the UN it estimated that for 2009 Global Criminal Proceeds may amount to US\$2.1 trillion,² (3.6% Global GDP) a figure which exceeds recent figures on illicit trade values of US\$1.79 trillion³ for the amount of black market crime, which is mostly made up from the proceeds from illegal drugs (approx US\$411bio), no longer the largest amount as now surpassed by proceeds from counterfeiting and piracy -- prescription drugs, food, clothing, shoes, luxury brands, movies, music, electronics, machine parts and currency (US\$691.5bio), by human trafficking, -- slavery, prostitution, economic migration, child exploitation (US\$240bio), and smuggling -- oil and gas, alcohol, tobacco and weapons (US\$162bio), and by illegal gambling -- illegal casinos and card clubs (approx US\$140bio).



These figures could even underestimate the problem, if you also add in Corruption and Fraud. The World Bank has estimated the amount of bribes paid at between US\$1 trillion to US\$1.6 trillion for example.⁴ Whilst there appear few reliable estimates for Fraud, it is clear that significant sums are lost, perhaps as much as US\$2.75 trillion, if you apply available estimates for both the UK⁵ and the US⁶ to other countries. These figures provide a stark reminder of the dangers to societies of 21st Century Crime

Organised and able to operate effectively across borders, criminals pursue these activities because they generate huge profits. They target markets where demand is strong and wealth is greatest. This means focusing on consumers in countries generating the most economic activity.



Whatever the true numbers, they are large and require a formidable response. It is axiomatic that governments need to design and implement effective measures to reduce both supply of criminal activities and demand for the products and services derived from such activities. However, governments have not succeeded in rolling back global criminal enterprises or successfully addressing the amounts laundered. According to the UN that estimated Global Criminal Proceeds of US\$2.1 trillion, in 2009 they also estimated that money flows laundered was estimated at US\$1.6 trillion and that money flows related to transnational organised crime was estimated at US\$870bio of which US\$550bio was available for laundering through the financial system. Approximately only US\$3.1bio or 0.2% of this amount is being seized.⁷ According to US Senator Carl Levin, as far back as 1999, “estimates are that US\$500bio - US\$1 trillion” are moved internationally “and that half of that money comes to the US”.⁸

On the supply side, much has been tried but little has proven to be sufficiently effective. Numerous individual successes can be claimed, but once an organisation is broken, or a leader imprisoned, another quickly takes their place. Precious little has been done to address the demand side of the problem. In response to the challenges faced by conventional law enforcement efforts aimed at limiting supply and apprehending criminals engaged in criminal activity, attention has shifted to identifying, tracing and seizing the proceeds of crime as they make their way through the illicit economy to the legal one. “Follow the money” is a common term today, but several decades ago

phrase and practice was a novel one born out of the difficulty governments were having in tackling criminal enterprises by focusing solely on their criminal acts. This fight against money laundering -- or anti-money laundering (AML) -- necessarily focuses on the financial system and the legitimate financial institutions that operate it.

The first war against drugs.

The history of combating drug trafficking is an instructive case study for the advent of AML. A hundred years ago, at the US’ behest, the great trading nations of the world came together, and finally agreed to criminalise the production and distribution of opium. The trade in opium had generated huge profits for trading companies and for States through taxation (none more than for the British Empire). However, the increasing addiction rates of populations, the deleterious effect on productivity, and the immorality of this enterprise led to the signing of the Hague Convention in 1912,⁹ hailed as a remarkable breakthrough when it came into force as part of the Treaty of Versailles in 1919 at the end of the First World War. The focus on supply-side prohibition of opium after significant insatiable demand had been established would be a policy response repeated when other drugs, like cannabis, amphetamines and cocaine, were made illegal.¹⁰

Notwithstanding the repugnance of the drug trade and the good intentions behind delegitimizing it, the net effect of withdrawing supplies of opium to millions of addicts was the creation of a massive illegal market, with huge profits to be made by producers and traders who were prepared to provide illicit supply. This should not have been a surprise, as this very outcome was predicted by British Prime Minister William Gladstone (who liked to take a drop of opium in tea often before giving a speech) in an earlier self-serving defence of the British government’s support for its own Empire’s addiction to taxes levied on the opium trade when he said “[Opium] prohibition would unleash organised crime, allow others to step in and further the insatiable demand for [drugs].”¹¹

The organised crime syndicates that followed have prospered and become transnational, controlling illegal drug production, transit and distribution. The last 100 years have seen illicit drug supply increase and expand in terms of substances (from opiates to narcotics and so-called psychotropic substances), size, and geographical scope. The organised transnational and local criminal enterprises that operate the drug trade also have expanded into new areas of illicit activity, cited above.¹¹

Advent of AML

To respond to the burgeoning narcotics trade, more than 25 years ago, the “follow the money” idea was conceived and embraced by governments of all shades, leading in 1988, to the Vienna Convention¹² that required “all members to adopt all necessary measures to enable confiscation of criminal proceeds from illegal drugs.” One year later, the Financial Action Task Force (“FATF”) was established by the then G7 group of nations to promote global standards on money laundering prevention. FATF has since extended its focus from drug trafficking to corruption, terrorism financing, WMD Proliferation Finance and other major crimes, that, also now include tax crimes. The idea is a simple one: focus on the money flows, the working capital, and the profit from serious crimes, in order to catch the criminals, to materially disrupt their criminal activities, and to create effective disincentives that will reduce serious crime.

Focusing on the financial proceeds of crime, as opposed to the underlying criminal activity, required fresh thinking, new methodologies and new players. FATF recognised the necessity of novel laws and regulations, as well as unprecedented co-operation among sovereign countries, their numerous law enforcement bodies and the financial services industry. Enlisting the financial sector was critical because it was assumed that criminals used banks and other financial intermediaries extensively – first introducing criminal proceeds into the sector (placement), then moving these funds to disguise their illegitimate origin (layering) and finally laundering their funds to obscure their illicit origin (integration).¹³ It was presumed that banks, exercising reasonable diligence, would be uniquely able to spot criminals and their financial activity. To help accomplish this, laws were passed requiring banks and others to introduce money laundering prevention programmes based on (i) knowing their customers -- identification and due diligence – (ii) monitoring of transactions to detect suspected criminal activity, and (iii) reporting such activity to government agencies that would launch investigations, prosecutions and seize financial assets.

According to criminologists, a rational person will only commit a crime if he believes the benefits outweigh the costs. In other words, to effectively deter criminal activity the probability of apprehension and conviction times the projected severity of punishment (including forfeiture of gains) must exceed the expected rewards. The hope behind AML efforts was that banks and others could provide enough information to law enforcement authorities who would follow up with successful prosecutions and asset seizures that would check the growth of, and potentially reduce, serious crime.

The first 25 years

Contrary to the perception in some quarters that financial institutions have not done much to prevent criminal enterprises from abusing their services, banks have made significant contributions, perhaps as much as US\$18bio¹⁴ both in terms of the billions of US\$ they have spent and the effectiveness of their actions. All reputable financial institutions, recognise they have an important role to play in combating money laundering, and they support the general strategy charted by governments.

Banks have worked tirelessly with governmental authorities, and international and national standard-setters, to establish and invest in programmes as new threats emerge and priorities change from drug trafficking and organised crime (where measures have increased the risks of detection and the costs of criminal activity) to corruption committed by so-called kleptocrats, who have found their access to the formal financial sector certainly impeded. Extensive efforts have been dedicated to combating terrorism finance and WMD proliferation finance, where automated systems and detailed knowledge of customers and transactions can provide crucial information quickly in response to governmental requests. With respect to the introduction of smart economic sanctions and embargo measures, the involvement of financial institutions has been critical to isolating rogue states and individuals from the formal financial sector. At the same time, the amount of information, in the form of Suspicious Activity Reports (SARs), filed by Banks and others in the industry has risen, year on year, to a level approaching 2 million individual reports a year.¹⁵

These are impressive results and the result of investments made in designing and implementing serious programmes to support the authorities in the fight against money laundering, corruption, terror finance, WMD proliferation finance, sanctions compliance and other serious crimes.

It would be incorrect and unfair to use enforcement proceedings against individual banks to detract from the overall performance and contributions made by the financial industry.

From 1989 to end-2013 financial penalties incurred by financial institutions for failure to comply with money laundering related laws, regulations or expectations, including for sanctions, violations, market abuse and fraud have topped US\$23.45bio, with more than half coming in the last 5 years.¹⁶

Without excusing some serious cases at Financial

institutions, it is predominantly weaknesses in implementing and complying with complex AML regulations that is the main issue and not aiding and abetting criminal activity. It is the criminals that should remain central to our concerns. Beyond gains achieved in the areas of terror finance, WMD proliferation finance, and Sanctions Compliance, the substantial efforts of banks have not resulted in the expected gains by others.

According to the “follow the money” strategy, information provided to governmental authorities by the banks and others should lead to prosecutions and asset seizures. With almost 2 million Suspicious Activity Reports (SARs) filed annually, there is no shortage of information. Nevertheless, despite these opportunities, asset seizure and forfeiture rates remain significantly below any form of tipping point. Whilst consistent figures are scarce albeit thankfully climbing in many countries (albeit flattered by forfeiture levies on financial institutions) so is the haul by criminals of the proceeds of crime.

According to the UN based on all available estimates, less than 1% of the total amounts that are being laundered are detected. The UN report issued in 2011¹⁷ found and reported that, “Data collected by the US State Dept suggest that some US\$3.1bio were seized in connection with money laundering activities in 32 countries out of 62 analysed (2010 or latest data available); more than 80% of this was seized in North America. This would be equivalent to some 0.2% of the best estimate of the extent of money laundering at the global level. In comparison, more than 20% of the globally produced opiates are being seized and more than 40% of cocaine.”

Other figures indicate the seizure rates, particular over the last few years are actually much higher than those reported in the UN study, particularly in the US¹⁸ but also elsewhere¹⁹ though recent increases are not as large. There is evidence however that increases are being made by the targeting of big ticket corporate fraud and bank enforcement cases which are overshadowing recoveries from the original targets being serious and Organised crime, particularly in the US. In Europe the picture is mixed. Whilst there is relatively little seized and forfeited in many European Countries a recent €1.6bio success against the Italian Mafia, by the Italian authorities is cause for optimism.²⁰

Despite some success it appears that few of these directly relate in some way due to the filings from SARs or at least there is little or no evidence to suggest that this is the case, or that the majority of the seized assets are in

the form of banked assets. For example, it is likely that most of all seizures are in the form of physical assets, such as real estate, businesses and cash, or from financial institutions’ forfeiture fines.

In sum, although the situation would have been worse without the last 25 years of anti-money laundering efforts and certain costs have been imposed on offenders, the cost-benefit calculus would appear to still tip decisively in favour of the criminal. Criminals enjoy not only a tax free income, but can expect to retain almost all of their illicit bounty. With large new markets to exploit, both geographic and industrial, the benefits to criminals in committing crime for profit remain compelling and growing.

The next 25 years

In response to the current situation, authorities have called for more of the same. In 2010, UNODC Head Antonio Mario de Costa reiterated his support for this strategy with the words,²¹ “Criminals are motivated by profit, so let’s go after their money,” and in 2012 FATF announced revised recommendations²² extending the “follow the money” approach, essentially increasing the ask on banks for the future even further. But there is no reason to believe that this will lead to materially improved results. Indeed, extension and intensification of the existing strategy may compound difficulties and make the effort, less efficient and no more effective than today.

What can be done is a genuine evaluation of “effectiveness”. FATF have indeed recognised this and deserve praise for not only making compliance with FATF standards an important part of the next round of Mutual Country Evaluations but also by including effectiveness as a core element that will also be evaluated, this should enable FATF, its sponsors and members, to critically assess the effectiveness²³ of the “follow the money” strategy and develop recommendations for action.

In the US, new FINCEN Director, Ms Shasky Calvery who until 2010 held the position of Chief of the Asset Forfeiture & Money Laundering Section of the US Department of Justice has begun to ask the difficult questions. In a speech to the American Bankers Association/American Bar Association, Ms Calvery acknowledged that institutions are spending a great deal of time and money on compliance programmes, however, she raised questions whether the money being spent is being spent in the right ways. “Industry and others often ask questions such as how does industry effort on compliance risk compare with illicit financing risks and what is the delta between them.” These are

questions that need to be answered by regulators, law enforcement and industry” in order to answer these questions a “Delta Team” has been established.²⁴

Where FATF and the US are already leading others should follow by ensuring effectiveness is a key theme for 2013 and beyond, reaching out to all stakeholders including financial institutions, establishing their own “Delta Teams” and considering the following 5 Recommendations to effectively combat Money Laundering as part of their work.

5 Recommendations to Effectively Combat Money Laundering

Five Recommendations to “Effectively” combat Money Laundering	
1	Set and reach a target for asset seizures (for example, 5% or US\$100bio in 5 years): Focus urgently on implementing all necessary measures to remove obstacles.
2	New Regulations should apply fully also to non-banks, and ensure international consistency on critical areas, e.g., CID, PEPs, BOs, DNFBPs, Wires; and be subject to a cost benefit analysis
3	Information on Risks and Threats must be shared and communicated: National Threat Assessments published and tailored for use by FIs, predicate priorities identified, typologies and strategies communicated.
4	Encourage financial institutions (who must improve cultures of compliance) enhance risk based approaches and provide incentives
5	Educate Consumers targeting demand as well as supply to refrain from supporting criminal actors in purchasing decisions and in understanding the money laundering broader context

Recommendation 1

Asset Seizure Targets - Firm asset seizure targets could be set with regards to the proceeds of crime. At least 5% of criminal proceeds, approx US\$100bio should be the medium term goal (e.g. after 5 years). In order to achieve this, enforcement authorities will need to invest additional resources to investigate the information provided from reports already filed by financial institutions that should be a road map for prosecuting many more criminals and seizing criminal assets. As a start, public resources directly employed to these tasks should match at least those invested by the private sector and results should be published.

A detailed study of the problems faced and the impediments to success and recommendations to improve

asset seizure and forfeiture the system was conducted by Matrix Insight and released in July 2009, following a request by the European Commission.²⁵ These recommendations should be acted upon.

FATF's 2012 Best Practices on Confiscation and a Framework for Ongoing Work or Asset Recovery²⁶ and the EU's proposed Directive on freezing and confiscation of the proceeds of crime²⁷ are a start but by themselves will make little impact and will not address the problem.

Recommendation 2

Regulations should ensure consistency and subject to Cost Benefit analysis - The introduction of new Regulations concerning AML largely falls upon financial institutions, and within FIs on Banks. Non-Bank FIs²⁸ and non-FIs²⁹ identified as presenting real risks should accept greater responsibility and increase their contributions to match those of the Banks. The Banks should not be expected to provide assurance where regulation is required on third parties.

New regulations are targeted at perceived gaps or perceived risk areas in the money laundering frameworks rather than on any assessment or threshold test, for example a cost benefit or effectiveness test before introduction. In many cases it is unclear whether proposed changes will have any material affect on the underlying levels of crime or criminal proceeds and yet the costs of introduction and compliance are largely ignored.

Regulations are also introduced across jurisdictions often inconsistently. The complexity of trying to comply with international best practices and at the same time national regulations can create confusion, drive up unnecessarily compliance costs and raise complexity. Financial institutions operating globally should be entitled to rely on internationally accepted standards, recognising that such standards may have an element of gold plating.

For core issues, such as, without limitation, (i) the definition of "Customer" (ii) the definition of "beneficial ownership" and definitions such as (iii) PEPs, (iv) wire transfer standards and (v) agreement over types of and approaches towards non-FIs that should be regulated designated entities, these should be universally consistent.

Recommendation 3

Information on Risks and Threats must be shared and communicated - It has become a cliché that flow of information sharing should not be a one-way

street; governments should share information with financial institutions. However, after years of lip service, governmental authorities have made little progress. If governments want to promote successful collaboration to combat financial crime and achieve more impressive results, they must entrust financial institutions with more information. A robust National Risk and Threat Assessment identifying and prioritising risks and threats honestly is essential as well as identifying where FIs can and should provide assistance. Furthermore, financial institutions should be able to maintain appropriate records, share certain information amongst themselves and across borders, without any conflict with applicable data protection or other laws or regulations. This need not include any individual SAR filing made in another country, though the underlying case facts and details should be included.

Additionally, clear priorities should be set and announced as to the relative importance and targets of effort.

All agree that actions to be taken are inevitably risk-based, i.e. the areas that present the greatest risk should receive the greatest attention, this is impossible without specific information from governments on their priorities. Currently, because of this lack of information, financial institutions find themselves in a difficult situation and regulators seem unwilling to offer any guidance or safe harbours. If the government doesn't set priorities, or says that everything is a priority - which amounts to the same thing - then financial institutions cannot accurately assess their risks or concentrate their compliance efforts on those areas that pose the greatest risk, and regulators cannot focus their examination and enforcement efforts on those areas either.

If priorities are set and clearly communicated then banks can and will translate the government's priorities into compliance systems across their mix of products and services, assessing the risks that their various business lines present and designing compliance systems that address those risks.

At the same time, regulators will design examination and enforcement protocols designed to ensure that banks have in place procedures that will adequately identify and control the risks associated with money laundering and terrorist financing. But in order to have a risk-based system, banks must know which crimes or similar activities should be given the highest attention and how regulators will approach Banks judgements in this respect. Absent this information, the result is likely to be in many cases unfocused compliance that tries to catch everything and winds up missing too much of the

things that are most important.

Based on harms and threats it would appear reasonable to assume that terrorism finance and WMD proliferation finance are indeed major priorities for many governments, though again, these should be expressly confirmed and remaining priorities enunciated. Based on the amounts of criminal monies derived, there is a case for considering that Counterfeiting and Piracy should increase in priority. Other priorities for inclusion will likely include, Corruption (kleptocracy); Fraud (specific elements, for example VAT Tax Fraud, Cybercrime); Illegal Gambling; Drug Trafficking; Human Trafficking and Smuggling which together make up to 95% of likely criminal proceeds.³⁰

For each, tailored strategies should be developed and the existing one size fits all, with excessive reliance on financial institutions, KYC, Monitoring and SAR filing should be reconsidered.

Recommendation 4

Encourage Financial Institutions – financial institutions must focus on preventing and detecting criminal proceeds, as well as implementing applicable AML Laws and Regulations and ensuring an institutional "culture of compliance" exists which emphasises the important role banks play in maintaining the integrity of the international financial system, national security and corporate social responsibility.

Financial institutions should be encouraged to adopt a "risk based approach", in their design and implementation of AML programmes and should not be second guessed provided such programmes are reasonable and proportionate and ultimately reasonably effective, particularly absent published regulatory specificity.

Contributions by financial institutions should be recognised and where appropriate taken into account when assessing an institution's record particularly before imposing fines and penalties. Banks should be encouraged to treat AML compliance costs differently than regular business expenses (e.g., facilities costs) and more like important capital investments that promote profitability and critical public goods.

Banks that routinely dedicate resources to efficient and effective compliance should be given direct economic benefits – reduction of examination fees and other supervisory assessments, consideration in calculating capital, or tax advantages.

Recommendation 5

Educate Consumers - Someone must educate the public about the true cost of money laundering and how money laundering plays a fundamental role in facilitating the drug trafficker, the organised criminal, the fraudster and the terrorist. Money laundering is not a victimless crime. Whilst it does not have the trauma of a robbery or produce the damage resulting from violent crime, money laundering can only take place after a predicate crime (such as robbery or drug dealing) has taken place. Reinforcing the clear link may also persuade and incentivise otherwise law abiding citizens of the consequences of paying for counterfeit or smuggled goods, use of economic migrants as cheap labour, prostitution, drug taking or involvement in illegal gambling. The economics of crime are no different from the economics of trade and reducing demand will have just as much an impact as disrupting supply.

Conclusions and Final Remarks

Financial institutions operate on the front line on the right side of a just war on the proceeds of crime, on a battlefield that is constantly changing, against an enemy who remains cunning, elusive and very well resourced, without being provided with much useful intelligence and in constant concern over the risk of friendly fire. This is no way to win a war!

The battle is not yet lost and we have plenty of fight left in us, so let us join once more to address the weaknesses in the strategy and to try to work ever more closely together as banks, regulators, policy makers, law enforcement and governments focusing on the common enemy, criminals and proceeds of their crimes.

Facts & Figures

global 2012 GDP or the size of the World Economy
US\$70 trillion

total assets under management managed by top 500 FIIs
US\$62 trillion

Wolfsberg Group member banks total assets combined amounting to around a quarter of the total assets held by the World's top 1,000 Banks
US\$20.8 trillion

GDP or the size of the world's biggest economy, US
US\$14.9 trillion

total value of assets held on deposit in Banks
US\$11 trillion

tax fraud and tax evasion losses
US\$4.75 trillion

total value of banknotes and coin in circulation
US\$4.2 trillion

average daily turnover of FX transactions
US\$3.9 trillion

total assets under management managed by Blackrock, the largest financial asset management firm
US\$3.3 trillion

total amount of fraud proceeds
US\$2.75 trillion

total amount invested in Hedge Funds globally
US\$2.3 trillion

total amount of criminal proceeds
US\$2.1 trillion

GDP or the size of the 8th largest economy: Italy
US\$2.1 trillion

total Global Military Expenditures
US\$1.7 trillion

total amount of criminal proceeds laundered perhaps the world's 10th largest industry
US\$1.6 trillion

total amount of bribes paid
US\$1-1.6 trillion

total amount of criminal proceeds generated by Organised Crime
US\$870bio

total amount of money generated from Counterfeiting & Piracy
US\$691.5bio

largest market generating criminal proceeds, the US
US\$620bio

total amount of money generated from Drug Trafficking
US\$411bio

total amount of international money remittances in 2012 largely flowing via Money Services Businesses
US\$400bio

total amount of money generated from Human Trafficking
US\$240bio

total amount of money generated from Smuggling
US\$162bio

total amount of money generated from Illegal Gambling
US\$140bio

EU VAT fraud costs States lost tax revenues
US\$100bio

total amount of money generated from Environmental Crime
US\$83.5bio

total international trade in conventional arms
US\$60bio

illicit trade in Oil and Gas
US\$54bio

costliest man-made environmental disaster, for BP Oil Spill in the Gulf of Mexico (incl largest fine of US\$4.5bio)
US\$42-65bio (est)

largest corporate accounting fraud, Enron Corp
US\$40-45bio

illicit trade in tobacco
US\$40.5bio

The wealthiest Charity in the World, the Gates Charitable Foundation
US\$37bio

total value of wildlife smuggling & poaching
US\$32bio

largest amount of funds embezzled by a kleptocrat - President Suharto of Indonesia (1967-98)
US\$15-30bio

fines levied against FIIs since 1989 to end-2013
US\$23.45bio

costs and investments by FIIs in AML Programme
US\$18bio

largest Ponzi Scheme, Bernie Madoff's Ponzi Scheme
US\$10-17bio

value of authorised small arms & light weapons sales
US\$8.5bio

largest rogue trader losses by Jerome Kerviel at SG
US\$7.2bio

criminal proceeds seized by authorities in 2010
US\$3.1bio

largest diamond producing country, Botswana
US\$3.25bio

largest corruption related fines and penalties for UK's GlaxoSmithKline
US\$3bio

largest AML & Sanctions related fine for a financial institution - UK's HSBC
US\$1.96bio

total amount of money generated from kidnap and hostage taking
US\$1.5bio

total amount of money generated from forgery
US\$1.1bio

the largest recorded robbery, the Central Bank of Iraq
US\$1bio

total number of credit, debit and prepaid cards in circulation
1 billion

largest sanctions related fine for a financial institution, UK's Standard Chartered
US\$667mio

the worlds most expensive sale of a private property, the Villa Leopolda on the French Cote D'Azure
US\$650mio

paycheque in 1997 for Drexel star banker Michael Milken before being charged with racketeering charges
US\$550mio

the Cullinan Diamond is the largest and most expensive diamond ever found owned by De Beers and valued at
US\$400mio

total number of people using illegal drugs
176-329mio

estimated annual payout to Somali pirates for kidnap for ransom
US\$189mio

the most expensive painting sold at auction is Francis Bacon's portrait of Lucian Freud
US\$142mio

messages per day carried by SWIFT, the leading international interbank message network
15mio

the world's most expensive car sold at auction, a 1957 Ferrari Testa Rossa
US\$12mio

total thefts, largest in the world by country is US
6.2mio

suspicious activity reports (SARs) filed in 2011, nearing
2mio

the no of PEPs listed in the database from Dow Jones
478,000

costs for the AQ attack on America 9/11
US\$400-500,000

most expensive bottle of wine sold at auction, a 1947 Cheval Blanc Bordeaux
US\$300,000

the largest number of murders in the world is in Brazil
44,000

most Kidnapping for Hostage annually - Mexico
18,000

What is Money Laundering?

Introduction

Whilst the term “money laundering” was invented and used for the first time only in the 20th Century, money laundering as a practice goes back much further, for example, as long ago as 4000 BC, Chinese merchants found ways of moving their money around in order to avoid identification and confiscation by the rulers of the Chinese State.

Activities that are now predicate crimes, go back as far, as opium usage would have been practiced around this time too and also later in 640 BC coins were counterfeited by clipping alloys and using the shavings to make new coins, the case of Hegestratos’ Fraud in 300 BC,¹ Roman laws addressing forgery enacted around 80 BC, and slavery, terrorism, murder, smuggling and theft of course not at all uncommon throughout antiquity.

What is the origin and true meaning of the term “Money Laundering”?

Fast forward to the Twentieth Century, the term “money laundering” is often said to have originated during “Prohibition” and from the activities of US gangsters, who needed to find ways to disguise the origins of the large amounts of cash, often in small denominated coins, generated by the illegal import and sale of alcohol and other activities such as gambling and prostitution.

With the Banks’ likely suspicious if large amounts of coins were deposited and the storage of large amounts of money in low value coins a challenge they created businesses, one of which was slot machines, and another of which was laundromats, which of course took coins to operate the machines, and so could pass off the proceeds of crime as proceeds from legitimate businesses. So it is thought by some that the term “money laundering” was born.

One of the first modern examples of money laundering followed the conviction of America’s most wanted at the time, Al Capone. It was the conviction for tax evasion that seems to have led to others fearing the same fate, paying closer attention to the financial side of their criminal businesses and establishing money laundering operations that would protect them and make any prosecution much more difficult. Meyer Lansky a cohort of Al Capone and known as the mob’s accountant, came up with a scheme that would be copied by many in later years. Lansky not only established offshore accounts with foreign banks, away from the gaze of US

prosecutors, but he also borrowed from these Banks, receiving what looked like legitimate loans, backed by the deposited criminal monies. These loans could even be disclosed to the revenue service and a tax deduction declared if necessary. Even so this scheme and others, were not described using the term, “money laundering.”

Whilst some commentators reject this historical origin for the term, whilst accepting coin operated laundromats may have been used amongst other retail and cash intensive businesses, they prefer a descriptive genesis for the term. For example, Jeffrey Robinson in his 1995 “The Laundrymen” where he considered money laundering mainly the proceeds of drug trafficking was the third largest industry in the world behind foreign exchange and oil and gas, (this is clearly an overstatement, see below), he also alleged that much of the laundered money was reinvested throughout the world by otherwise legitimate businessmen, lawyers, accountants and bankers, describing why it is called as it is, as follows:

“Money laundering is called what it is because that perfectly describes what takes place - illegal, or dirty, money is put through a cycle of transactions, or washed, so that it comes out the other end as legal, or clean, money. In other words, the source of illegally obtained funds is obscured through a succession of transfers and deals in order that those same funds can eventually be made to appear as legitimate income”.²

.....Jeffrey Robinson, “The Laundrymen”

Whilst the arguments over the origin of the term will continue, money laundering as a term of expression appears to have been used first, at least as far as we can tell from records available, as part of the reporting of the Watergate scandal in the early 1970s.

Investigating, the burglary of the Democratic National Committee Headquarters in Washington’s Watergate building on 17 June, 1972, Washington Post reporters, Bob Woodward and Carl Bernstein, chronicled in All the President’s Men, broke the story that led to the resignation of then US President Richard Nixon.

The reporters learned that investigations carried out by Miami Dade County chief investigator Martin Dadis uncovered a cashier’s cheque for US\$25,000 deposited into a Boca Raton bank account of one of the burglars, Bernard Barker. Dadis had subpoenaed the Boca Raton bank records upon learning that Barker was carrying more than US\$5,000 in new, consecutively numbered US\$100 bills when he was arrested. Dadis followed the new bills back to the Boca Raton bank and uncovered the US\$25,000 cheque payable to Ken Dahlberg deposited in Barker’s account. The reporters pursued

the Dahlberg connection and learned Dahlberg was the Republican’s Midwest finance chairman of Nixon’s 1972 re-election campaign. Dahlberg had collected US\$25,000 in cash from a Nixon re-election donor who wished to remain anonymous in order to avoid disclosing the contribution under the new campaign financing laws.

Dahlberg converted the cash into a cashier’s cheque payable to himself and gave the cheque to Maurice Stans, finance chairman for the Nixon campaign. Dardis explained that the new campaign finance law that came into effect on April 7 1972 had triggered a massive effort by Stans to solicit re-election contributions from donors. Stans would tell reluctant donors that if they didn’t want their contributions traced back to them, their anonymity could be ensured by moving their contributions through Mexican banks because Mexico does not allow the US to subpoena bank records. Dardis explained, “It’s called laundering. You set up a money chain that makes it impossible to trace the source. The mafia does it all the time. So does Nixon...This guy Stans set up the whole thing.”³

This system allowed Nixon’s re-election campaign to receive illegal contributions from corporations, and other impermissible or illicit donor groups. Stans used Banco Internacional in Mexico City for the scheme and it was Banco Internacional that issued the US\$25,000 Dahlberg cashier cheque.

As a result an article appeared in the Washington Post on 1 August 1972 headlined: “Bug Suspect Got Campaign Funds”. The story immediately triggered three separate investigations and helped seal Nixon’s fate. As one Post reporter commented: “It [the cheque] was the first real connective glue between Watergate, its funding and the Nixon campaign.”⁴

The expression first appeared in a formal context, in a US court in 1982 in the case US v US\$4,255,625.39 (1982) 551 F Supp.314. This matter involved a forfeiture case, where it was decided that over US\$4mio in cash currency plus the balance on a bank account in Miami of more than US\$3.6mio could be seized, as a “substantial connection” between the money and narcotics transactions was made. The court in its judgement mentioned the fact that, “Miami has become a centre for drug-smuggling and money laundering.”⁵

Money laundering was first criminalised in the US in 1986 with the passing of the Money Laundering Control Act. In the 1986 Act Money Laundering was described as:

“between money laundering and organised crime. Congress’s primary intent was to criminalise the, ‘process by which one conceals the existence, illegal source, or illegal application of income, and then disguises that income to make it appear legitimate.”

.....US Money Laundering Control Act 1986⁶

In 1988 in the UN Convention against illicit traffic in narcotics and psychotropic substances, also known as the Vienna Convention was the first international instrument which included in its purposes criminal asset forfeiture in order to combat serious crime and Money Laundering was defined as:

“the conversion or transfer of property, knowing that such property is derived from any (drug trafficking) offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions; the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses; the acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses..or from an act of participation in such offense or offences.”

.....UN Vienna Convention 1988⁷

In 1999 the UN in its International Convention for the Suppression of the Financing of Terrorism defined “terrorism financing” as follows:

“Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out” (a) An act which constitutes an offence within the scope of and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970.”

.....United Nations 1999 International Convention for the Suppression of the Financing of Terrorism⁸

The money laundering definition used in the Vienna Convention remains current and are referenced as the standard by FATF in its 2012, 40 Recommendations, where it states

“FATF incorporate the Vienna Conventions technical and legal definition of Money Laundering and recommends ex-

panding the predicate offences to include all serious crimes.” It also states the following in the 40 Recommendations in 2012 referring money laundering to

“The processing of...criminal proceeds to disguise their illegal origin in order to legitimise the ill-gotten gains of crime.”⁹

FATF also include a definition of Terrorist financing which is:

“Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organisations.”

.....FATF 2012, 40 Recommendations⁹

Other Definitions or Descriptions of Money Laundering / Terror Financing

The following are a selection of definitions and descriptions of “money laundering” and “terror finance” from all over the world:

“the conversion or transfer of property, knowing that such property is derived from serious crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in committing such an offence or offences to evade the legal consequences of his action, and the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from serious crime.”

.....Article 1 EU First Money Laundering Directive 1991¹⁰

“Money Laundering is the process by which criminal proceeds are sanitised to disguise their illicit origins. Acquisitive criminals will attempt to distance themselves from their crimes by finding safe havens for their profits where they can avoid confiscation orders, and where those proceeds can be made to appear legitimate. Money laundering schemes can be very simple or highly sophisticated. Most sophisticated money laundering schemes involve three stages: Placement - the process of getting criminal money into the financial system; Layering - the process of moving money in the financial system through complex webs of transactions, often via offshore companies; Integration - the process by which criminal money ultimately becomes absorbed into the economy, such as through investment in real estate. Prosecutions for money laundering can involve any of these stages in the money laundering process.”

.....UK Proceeds of Crime 1992 Preamble¹¹

“The basic characteristics of the laundering of the proceeds of crime, which to a large extent also mark the operations of organised and transnational crime, are its global nature,

the flexibility and adaptability of its operations, the use of the latest technological means and professional assistance, the ingenuity of its operators and the vast resources at their disposal.”¹²

.....UN report 1993¹²

“Money laundering is the process of making illegally-gained proceeds (i.e. “dirty money”) appear legal (i.e. “clean”).

Typically, it involves three steps: placement, layering and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the “dirty money” appears “clean.” Money laundering can facilitate crimes such as drug trafficking and terrorism, and can adversely impact the global economy.”

.....FinCEN¹³

“Money Laundering is broadly interpreted as feeding the proceeds of crime or corruption into the financial system in order to give it the appearance of proceeds of legitimate activity, and the financing of illegal activities including terrorism through financial systems.”

.....UBS Global AML Policy since 2004¹⁴

“... (i) the conversion or transfer of property derived from criminal activity to conceal or disguise its illicit origin; (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of property known to have been derived from criminal activity; (iii) the acquisition, possession or use of property known to have been derived from criminal activity; (iv) the participation, or assistance, in the commission of any of the activities above.”

and.... “terrorist financing” means the

“provision or collection of funds to carry out any of the offences defined in Council Framework Decision 2002/475/JHA on combating terrorism, such as hostage taking, the drawing-up of false administrative documents and the leadership of a terrorist group.”

.....EU Third Money Laundering Directive 2005¹⁵

“Money laundering is the conversion of the proceeds of criminal activity into apparently clean funds, usually via the financial system. This is done by disguising the sources of the money, changing its form, or moving the funds to a place where they are less likely to attract attention. “Criminal activity” includes fraud, corruption, drug dealing and other serious crimes.”

.....EU press Release 2012¹⁶

“Money laundering is the attempt to conceal or disguise the nature, location, source, ownership, or control of money.”

.....MoneyGram¹⁷

“Money laundering is the covert introduction of illegally acquired assets into the legitimate economy with the aim of disguising their true illegal origin.”

.....Swiss Bankers Association¹⁸

“Legitimisation (washing) of illegally obtained money to hide its true nature or source (typically the drug trade or terrorist activities). Money laundering is effected by passing it surreptitiously through legitimate business channels by means of bank deposits, investments, or transfers from one place (or person) to another.”

.....BusinessDictionary.com¹⁹

“money laundering is any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources.”

.....Interpol²⁰

“Disguising the source of money generated through illegal activities so that it resembles legitimate income. Money laundering involves breaking up large amounts of cash into smaller transactions, changing its form through investments or deposits into bank accounts, and moving the money through seemingly legitimate businesses to bring it into mainstream economy.”

.....Nasdaq²¹

“Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets.”

and

“Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organisations....Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.”

.....FINRA²²

“The attempt to conceal or disguise the ownership or source of the proceeds of criminal activity and to integrate them into the legitimate financial systems in such a way that they cannot be distinguished from assets acquired by legitimate means. Typically this involves the conversion of cash-based proceeds into account-based forms of money.”

.....OECD²³

“Money laundering is the name given to the process by which illegally obtained funds are given the appearance of having been legitimately obtained.”

.....Austrac²⁴

“Money Laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins...involving the proceeds of criminally derived property rather than the property itself.....and Financing of terrorism is the financial support in any form of terrorism or of those who encourage, plan, or engage in it.”

.....The World Bank²⁵

“Terrorist financing refers to the processing of funds to sponsor or facilitate terrorist activity. A terrorist group, like any other criminal organisation, builds and maintains an infrastructure to facilitate the development of sources of funding, to channel those funds to the providers of materials and/or services to the organisation, and, possibly, to launder the funds used in financing the terrorist activity or resulting from that same activity. Terrorist organisations derive income from a variety of sources, often combining both lawful and unlawful funding, and where the agents involved do not always know the illegitimate end of that income. The forms of financing can be grouped in two types: Financial support – In the form of donations, community solicitation and other fundraising initiatives. Financial support may come from states and large organisations, or from individuals. Revenue generating activities - Income is often derived from criminal activities such as kidnapping, extortion, smuggling or fraud. Income may also be derived from legitimate economic activities such as diamond trading or real estate investment.

The terrorist financier will want to disguise the illegal end of the funds, while trying to maximize the revenues for the organisation sponsored. It may be necessary to disguise the source of the funds, as well, either because such funds have an illegal origin, or because the organisation wants to preserve the continuity of the legitimate financing. The need to camouflage the source of the funds means that terrorist financing has certain similarities with traditional money laundering, namely the use of three stages to place, layer and integrate the funds in the international financial system.”

.....Fides²⁶

“Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the money can lose its criminal identity and appear legitimate. Illegal arms sales, smuggling, and the activities of organised crime, including for example, drug trafficking and prostitution, can generate huge sums. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits

and create the incentive to “legitimise” the ill-gotten gains through money laundering. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention. In summary, the money launderer wants to: place his money in the financial system, without arousing suspicion; move the money around, often in a series of complex transactions crossing multiple jurisdictions, so it becomes difficult to identify its original source; and then move the money back into the financial and business system, so that it appears as legitimate funds or assets.”

..... Financial Supervision Commission Isle of Man²⁷

“Terrorist financing involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organisations. Funds may stem from both legal and illicit sources. More precisely, according to the International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism “if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out” an offence within the scope of the Convention. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.”

..... IMF²⁸

“The process of creating the appearance that large amounts of money obtained from serious crimes, such as drug trafficking or terrorist activity, originated from a legitimate source.”

..... Investopedia²⁹

And many more.....

What are the stages of “Money Laundering”?

So much for the origin of the term “Money laundering” but what is it? According to FATF, money laundering is made up of the following 3 stages;³⁰ placement, layering and integration

Placement

In the initial - or placement - stage of money laundering, the launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders,

etc.) that are then collected and deposited into accounts at another location.

Layering

After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not cooperate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

Integration

Having successfully processed his criminal profits through the first two phases the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

.....FATF 2012, 40 Recommendations

This 3 stage process, the classic description of money laundering has also been described as “immersion”; generally inserting the proceeds of crime into the legitimate financial system, “heavy soaping” or disguising the trail of the monies as they pass through the financial system and finally the “spin dry” when the funds make it into legitimate income or assets.

Furthermore FATF explain where Money Laundering may occur as follows:³¹

“As money laundering is a consequence of almost all profit generating crime, it can occur practically anywhere in the world. Generally, money launderers tend to seek out countries or sectors in which there is a low risk of detection due to weak or ineffective anti-money laundering programmes. Because the objective of money laundering is to get the illegal funds back to the individual who generated them, launderers usually prefer to move funds through stable financial systems.

Money laundering activity may also be concentrated geographically according to the stage the laundered funds have reached. At the placement stage, for example, the funds are usually processed relatively close to the underlying activity; often, but not in every case, in the country where the funds originate.

With the layering phase, the launderer might choose an

offshore financial centre, a large regional business centre, or a world banking centre – any location that provides an adequate financial or business infrastructure. At this stage, the laundered funds may also only transit bank accounts at various locations where this can be done without leaving traces of their source or ultimate destination.

Finally, at the integration phase, launderers might choose to invest laundered funds in still other locations if they were generated in unstable economies or locations offering limited investment opportunities.”

For Terrorism Finance, FATF, in their 2008 Terrorism Financing Typologies Report, also highlighted 3 stages, though these were not Placement, Layering and Integration, but Raising, Moving and Using funds, both criminally originated funds, where the 3 money laundering stages would still apply, but also to legally originated funds

What is the size of “Money Laundering”?

Money Laundering may be the 10th Largest Industry in the World and one of the most profitable.

It is often quoted and considered as conventional wisdom that money laundering is the third largest industry in global terms behind foreign exchange and oil and gas. In fact, this is clearly overstating its size, with Food, Retail, Energy including Oil and Gas, Financial Services, Tourism, Manufacturing including Automobiles, Telecommunications and Pharmaceuticals/healthcare all substantially larger. Money Laundering is also likely behind also the Arms Industry, but may still just make it into the top 10 at number 10.

Top 10 Global Industries	
1	Food
2	Retail
3	Energy
4	Financial Services
5	Tourism
6	Manufacturing
7	Telecommunications
8	Healthcare
9	Arms & Defence
10	Money Laundering

Source: Author

Despite its position as perhaps the 10th largest, there is little doubt that it is one of the most profitable with

huge margins and of course all proceeds are tax free. According to the UN for 2009, out of US\$2.1 trillion in criminal proceeds, approximately US\$1.6 trillion was laundered but only US\$3.1bio was seized, giving an effective tax or clean up rate of 0.2%.³²

The figure of US\$2.1 trillion is a figure that related to classic predicate offences. These numbers ignore bribery and corruption estimated at US\$1 trillion - US\$1.6 trillion a year,³³ As predicate offences also now include insider dealing and market manipulation, fraud and tax fraud, these figures could be increased further for fraud by as much as US\$2.75 trillion³⁴ and tax fraud and tax evasion as much as US\$4.75 trillion.³⁵

Final Comments / Conclusion

As criminal activity, beyond drug trafficking become classified as predicate offences to Money Laundering, the original definitions and the classical 3 stages are unlikely to be sufficient to fully describe what money laundering is and how it is carried out, particular when considering, trade based laundering schemes, insider dealing and market manipulation, terrorism finance, tax fraud and tax evasion. Furthermore with advances in technology, electronic and mobile cash and digital currencies, we may need to consider whether money alone remains the principal concern.



Section 1 - Money Laundering Crimes

- Introduction, 21
- Bribery & Corruption
- Counterfeiting & Piracy of Products, 29
- Drug Trafficking, 35
- Environmental Crime, 42
- Extortion, 48
- Forgery, 50
- Fraud incl Tax Fraud & Cybercrime, 52
- Human Trafficking, 63
- Illicit Arms Trafficking, 66
- Insider Dealing, 69
- Kidnap, Illegal Restraint & Hostage Taking, 78
- Market Manipulation, 82
- Murder and Grievous Bodily Injury, 89
- Organised Crime, 93
- Smuggling, 100
- Terrorism Finance, 106
- Theft, Robbery & Trafficking, 118
- WMD Proliferation Finance, 123

Introduction

The crimes that are included in this Part 1, Section 1, are those that have for many years been included in FATF's list of predicate offences to Money Laundering, as well as the most recent additions which together are seen as the most serious criminal offences which need to be countered.

FATF designated categories of offences include	
1	Participation in an organised criminal group and racketeering
2	Terrorism including terrorism financing
3	Trafficking in human beings and migrant smuggling
4	Sexual exploitation including sexual exploitation of children
5	Illicit trafficking in narcotic drugs and psychotropic substances
6	Illicit arms trafficking
7	Illicit trafficking in stolen and other goods
8	Corruption and bribery
9	Fraud
10	Counterfeit and piracy of products
11	Environmental crimes
12	Murder, grievous bodily injury
13	Kidnapping, illegal restraint and hostage taking
14	Robbery or theft
15	Smuggling (including in relation to customs & excise duties and taxes)
16	Tax crimes (related to direct taxes and indirect taxes)
17	Extortion
18	Forgery
19	Piracy
20	Insider trading and market manipulation

Source: FATF 40 Recommendations 2012¹

Whilst most are crimes which have a financial gain as the motive, some may not, for example, murder and bodily harm, though in an organised crime context violence is part of the necessary tool box required to stay in business and effective, or terrorism which is politically motivated, though requires funding often generated from the proceeds of crime but in other cases

is funded from legitimately sourced funds.

Whilst all these serious crimes threaten individuals and society's health and prosperity in varying degrees, the levels of activity, the criminal profits that are generated, the numbers of persons involved in criminal acts and the degree of harm caused as a result make any relative comparison or list which prioritizes these crimes based on negative consequences extremely challenging.

Whilst aggregated statistics are scarce the following, according to Havocscope, generate the most in criminal proceeds:

Criminal Proceeds by Crime		
No	Activity	US\$ Proceeds
1	Bribery & Corruption	1-1.6 trillion
2	Organised Crime	870bio
3	Counterfeiting & Piracy	691.5bio
4	Drug Trafficking	411bio
5	Human Trafficking	240bio
6	Smuggling	162bio
7	Illegal Gambling	140bio
8	Environmental Crime	83.5bio
9	Kidnap & Ransom	1.5bio
10	Forgery	1.1bio

Source: 1 - World Bank² / 2-10 - Havocscope³

Havocscope focuses on Black Markets, and largely ignores "Fraud" which is a very broad category of offences, sometimes described as "White Collar Crime" and whilst no aggregate number is available, it could be that in total this number could exceed all other Black Market crimes.

Looking at how the International Community responds, it can be assumed that Terrorism and Terrorism Finance together with WMD Proliferation remains at the top of the list. Whilst Terrorism itself is shocking and the mayhem caused deeply disturbing for those involved, its impact beyond grabbing media headlines is limited. Nevertheless, it is where Terrorism and WMD Proliferation come together that the potential for harm on an almost unimaginable basis provides greatest concern. It is also why so-called "Rogue States" engaged in developing WMD also cause greatest concern. Whilst the traditional view of terrorism was that terrorists would seek to limit casualties so as to make an impact but not to cause an excessive damaging

response, the events of 9/11 changed that view. Though the traditional view may still hold for the majority of the major terrorist organisations, Al-Qaeda has clearly departed from that view and only the complacent would consider Al-Qaeda as either a spent force or unwilling if it had the means to use WMD.

Following Terrorism and WMD, Drug Trafficking and with it those organised criminal gangs involved would appear to be the next biggest priority, at least if judged by the amount of effort and resources still deployed and expended since the so called "War on Drugs" began in the 1970s. Whilst the War on Drugs and the focus on Organised Crime has had notable individual successes, the criminal supply lines are strong and enduring and those involved continue to grow their criminal businesses.

Next is hard to tell. Corruption receives a lot of attention, including from Policy Makers, Academics and the Media, though in practice on the ground progress is slow and Corruption remains endemic in many parts of the World and for many it is a way of life.

Smuggling and more recently Tax Fraud, where governments lose billions to criminals and to otherwise law abiding citizens in evading taxes also receives a lot of attention and appears to be an increasing real priority.

Human Trafficking has also begun to receive more attention and appears to be increasingly a priority issue.

For the rest these would appear to remain important but lack the appeal or the focus that is attached to terrorism or corruption, for example. It is interesting that according to sources, the crime that generates the most in illegal profits, counterfeit and piracy, even more than for drugs appears to have a relatively speaking low priority.

The fifth most profitable crime generating criminal profits according to Havocscope is illegal gambling which is not listed by FATF as a predicate or serious crime.

Bribery & Corruption

"We know what corruption has cost us – it has denied us the value of our resources, both human and natural. It breeds injustice. It causes killings. It causes diseases that ravage us everywhere"

Nuhu Ribadu, Head of Nigerian Economics and Financial Crimes Commission. 2006¹

Harms

There is no shortage of evidence as to the debilitating impact corruption has on society. It is indeed a cancer, as Senator Frank Church stated in 1976 and was reiterated some twenty years later by the former President of the World Bank James Wolfensohn.

Corruption thrives on weak institutions, political instability and vulnerability. It undermines democracy and the rule of law, leads to violations of human rights, distorts markets, erodes the quality of life and allows organised crime, terrorism and other threats to human security to flourish. Corruption blights countries, infects industries and raises the costs of living and commerce.

The economic damage and human misery that corruption can cause is visible in countries as seemingly diverse as those states where levels of corruption by, for example, Transparency International are considered comparatively high for example in the Euro zone such as Greece and Italy; countries devastated by long-term low-level warfare such as Afghanistan and Pakistan, and countries that are economically booming such as China and Malaysia.

Statistics

Estimating the dimensions of the money flows related to corruption either in terms of how much is paid or how much is laundered as the profits of bribery is virtually impossible. Still the World Bank in 2004 estimated that the annual total of bribes paid worldwide was US\$1 trillion² and the UN later in 2009 stated that political corruption costs up to US\$1.6 trillion.³

The World Bank also reported in 2012 that between US\$20-40bio is lost to corruption and other crimes each year in developing countries, amounting to some 20-40% of all international aid sent to developing countries each year.⁴

Transparency International Indices

Transparency International (TI) is a non-government organisation formed in 1993, which monitors corporate and political corruption. It has developed a number of different methodologies to try and measure corruption,

including the Bribe Payers Index and Industries most prone to corruption, and the Corruption Perception Index.

TI The Bribe Payers Index ("BPI")⁵

The BPI measures the likelihood of companies from industrialized countries bribing abroad. The 2011 BPI report concluded that Dutch and Swiss firms were the least likely to bribe abroad, while Russian, Chinese and Mexican companies were the most likely.

TI Bribe Paying Industries

The 2011 Report also evaluated the industries most prone to corruption. Sectors are scored on a scale of 0-10, where a maximum score of 10 corresponds with the view that companies in that sector never bribe and a 0 corresponds with the view that they always do. Public works contracts and construction were the sectors whose companies were most likely to bribe abroad. The least likely industries were agriculture and light manufacturing.

TI Bribe Paying Industries to Public Officials	TI Scale
Public works contracts & construction	5.3
Real estate & property legal & business services	6.1
Utilities	6.1
Oil & gas	6.2
Mining	6.3
Pharmaceutical & health care	6.4
Power generation & transmission	6.4
Heavy Manufacturing	6.5
Arms & defence & military	6.6
Fisheries	6.6
Telecommunications	6.7
Transportation & storage	6.7
Consumer Services	6.8
Forestry	6.9
Banking & finance	6.9
Civilian aerospace	7.0
IT (computers/software)	7.0
Agriculture, Light manufacturing	7.1

Source: Transparency International 2011

TI Corruption Perception Index ("CPI")⁶

The CPI ranks countries and territories according to perceived levels of public sector corruption on a scale of 0 (highly corrupt) to 10 (very clean). The 2013 Corruption Perceptions Index shows that no region or country in the world is immune to corruption. The majority of the 183 countries and territories assessed scored below five.

In 2013, the least corrupt countries according to the CPI were Denmark, New Zealand, Finland, Sweden, Norway and Singapore. The most corrupt countries were Somalia, North Korea, Afghanistan, Sudan, South Sudan Libya and Iraq.

Definition / Description

There are many faces of corruption and no one universal definition. TI defines corruption as "the abuse of entrusted power for private gain", which is simple and straightforward but fails to take account of private forms of corruption. Bribery is perhaps the most easily recognised form of widespread corruption.

Corruption can be described by many terms, including, "kickbacks", "payoffs", "Baksheesh", "graft", "payoff", "hush money", "tips", "grease", "bung" and "sweeteners" and comes in many forms, including, "nepotism", "cronyism" as well as "extortion".

Corruption is a crime committed by at least two parties, the payer and the beneficiary, who is often the payee, but oftentimes with others involved, particularly intermediaries or nominees. Whilst Corruption is usually demand led, this is not always the case, as the payer may initiate or offer a bribe, particularly where the interests of the payer is at stake.

Corruption can involve at least 4 main forms: Petty Corruption, Private Corruption, Organised Corruption and Grand Corruption (see later under money laundering for details)

Historical Background / Context

Corruption has a long history. Whether it is thirty pieces of silver, the price for which Judas Iscariot was bribed to betray Jesus Christ, or the US\$15-35bio, the Former Indonesian President Mohammed Suharto is estimated by TI to have embezzled, our history is unfortunately littered with far too many examples of it.

Ruthless and corrupt feudal lords and nobility ruling the Holy Roman Empire in the 13th Century earned their name in history as Robber Barons, by abusing their authority and imposing unjust tolls to passing ships on the River Rhine. The term Robber Baron was later

popularised in American literature during the Great Depression describing ruthless businessmen and later the industrialists in the so called "Gilded Age".

Another early example of corruption is seen in the Roman Catholic Church in the early 16th Century with respect to the sale of indulgences. Indulgences were pieces of paper that gave pardon for sins. Salesmen appointed by the Church commercially exploited the sale of indulgences and proceeds were used to fund Crusades and Churches, including St Peter's Basilica. The level of Corruption would cause a protest movement to emerge following Martin Luther's stand against the Church, provoking the reformation and the schism in Christianity. Following the reaction, the sale of indulgences was eventually prohibited in 1567.

Examples of corruption in more modern times continue to cover the full spectrum, from petty, private, organised to grand. Some periods of modern history deserve particular mention:

The Post War Period

Following the defeat of Nazi Germany and Imperial Japan, Independence movements would shape a new destiny for many countries, previously occupied and/or subject to Colonial rule. At the same time a cold war emerged offering leaders of new independent nations opportunities to position their countries in a new form of relationship both with their previous Colonial Masters and to court the great powers now seeking influence and support. The struggle during the Cold War between left and right was fought all over the world, with particular hotspots in Asia, Africa, the Middle East and Latin America. So called Soviet Satellite States, would emerge for example, Angola and Cuba as well as those countries that were bound inside the Iron Curtain in Europe. Chinese Maoist influenced States such as North Korea, Vietnam, Laos and Cambodia would also emerge but would also lead to the Korean and Vietnam wars killing millions. In order to stop the march of Communism many leaders would be supported by the West, though in so doing, the West would also be complicit in their activities including the Grand Corruption that took place during their reigns.

In Asia for example, when Mohammed Suharto came to power in Indonesia, in 1967, he became Indonesia's second President, following the ouster of Former President Sukarno. Sukarno had ruled since leading the Independence struggle from the Dutch in 1949. Throughout Sukarno's tenure as President factions from both right and left jockeyed for positions with Sukarno moving to the left, closer to the Soviet Union and China and away from the West. When Communists tried in

1965 to take over the entire state Suharto as then Army Chief of Staff put down the insurgency and soon gained the Presidency for himself with the support of the West. In the Philippines, President Ferdinand Marcos was at first a popular President when he was elected in 1965, quickly deploying troops to support the US in Vietnam.

In Africa, for example, Mobuto Sese Seko was made President of Zaire (formerly the Belgian Congo) in 1965, following the assassination of President Lumumba. For more than 50 years there has been great controversy over his death with many believing that the CIA were involved. Western concerns over the political independence of Lumumba were real, whatever the truth is about the assassination. Zaire was sitting on massive deposits of commodities, including uranium that was the chief source of nuclear materials, from which both the Hiroshima and Nagasaki bombs had been created. Another example of where post Colonial and Cold War politics provided the space for Corrupt Leaders to flourish, include the cases of the Francophile, Omar Bongo in the Gabon, President from 1967 to 2009.

In Latin America, the ideological struggle that had long since existed in the region, between states and régimes supported by the US and those that did not between states turning left or right. Those Presidential Strongmen, like Augusto Pinochet in Chile who was president from 1973 until 1990 and the father and son Presidents of Haiti ruling from 1957 until 1986, Papa and Bebe Doc Duvalier; and Alberto Fujimori, President of Peru from 1990 to 2000 aided by his security chief Vladimiro Montesinos, to name just a few, were for a time strongly supported.

Military, diplomatic and financial support by the West directly assisted these leaders in staying in power and in committing human rights abuses and leading to conditions where Grand Corruption was possible.

The West, in many of these cases finally withdrew support or indeed actively brought them down, for example, in the case of General Manuel Noriega.

The US Foreign Corrupt Practice Act (FCPA) and Bribery of foreign officials in international business transactions.

The Watergate scandal in the 1970s revealed the wide spread existence of slush funds being used by American multinational companies in order to make illegal political contributions. This prompted the US SEC to investigate certain non-disclosed questionable payments made to foreign officials. As a result, between 1975 and 1976, a number of US Senate hearings took place that

looked into the questionable payments. Led initially by Senator Frank Church, the investigations revealed that the practice of bribing foreign government officials was widespread but not illegal under US law. Well known American multinationals, particularly from the arms and petroleum industries, including Gulf Oil, Exxon Corporation, Mobil Oil Corporation, Northrop Corporation, and Lockheed Corporation admitted to making bribe payments of millions of dollars to various government officials in Saudi Arabia, Italy, Honduras and Korea in return for favorable treatment.

Although it was not illegal under US law at the time to pay a bribe to a foreign official, the companies had nonetheless taken great measures to distance themselves from the recipients of the bribes by using offshore slush funds, fictitious expenses and third parties described as "marketing agents" or "foreign sales agents" to pay the bribes to government officials who themselves held accounts offshore.

It was estimated at the time that over 400 US companies were found to have made questionable payments totaling approximately US\$300mio. The business industry argued that such payments were essential to remain competitive and maintain market share, at a time when their European counterparts could deduct bribe payments for tax purposes. In response to the investigation and with particular concerns to foreign policy and fuelling a new arms race, legislation was drafted to address the bribery of foreign officials. After various attempts and proposals to reign in the questionable payments under a self disclosed voluntary regime, the FCPA was passed in 1977 which today, makes companies criminally liable for bribery to foreign officials, whether directly or via an intermediary and requires controls and accounting standards to detect and prevent bribe payments.

It took almost 20 years before the international community addressed foreign bribery in international transactions. In 1996 the Inter American Convention against Corruption was adopted by the OAS. This represented a regional consensus about what States should do in the areas of prevention, criminalisation, international co-operation and asset recovery. Following this in 1998, the EU Council of Europe Criminal Law and Civil Law Conventions were adopted. Then came the OECD Convention on combatting Bribery of Public Officials in International Business Transactions in 1999. This would be followed by the UN Convention against Corruption (UNAC) signed in 2003 as well as the African Union Convention on Preventing and Combatting Corruption also in 2003. In 2009 the OECD made more Recommendations for

further combatting bribery of Foreign Public Officials in International Business Transactions. Most recently, after much criticism of the UK, came the UK Bribery Act 2010 which is now seen as one of the very toughest Anti-Bribery Statutes in force.

Post Soviet Collapse.

When the Berlin wall came down in 1989 and the Soviet Union was dissolved, the Post Soviet era would lead to a radical transformation in Russia and former Soviet Republics. The rapid transformation in post communist Russia during the 1990s, for example, saw assets transferred from public to private ownership via voucher privatization, loans for shares schemes and other auction schemes resulting in the rise of the Russian Oligarchs.⁷ At a time when approximately 40% to 50% of the population was living in poverty, the Oligarchs became billionaires through powerful government figures and through access to finance desperately needed by the Russian state. This resulted initially in a handful of individuals controlling Russia's major companies, particularly the natural resources industry and major newspapers and TV stations. These Oligarchs have often been likened to America's Robber Barons who also amassed great fortunes but also where they were for a time, questioned and where some fell foul of the law.

Arab Spring

The Arab Spring movement, which began in December 2010 has again focussed the world on leaders who acted as dictators, in Egypt, Libya and Tunisia. The exact amounts of stolen assets involved in the cases of Zine al-Abidine Ben Ali (Tunisia), Hosni Mubarak (Egypt) and Muammar Gaddafi (Libya) are still being determined, however, parallels between these modern day Kleptocrats and past cases of corruption can easily be drawn. These Former leaders of Egypt, Libya and Tunisia, together with their families and close associates are all alleged participants of endemic corruption, self enrichment and gross misuse of state funds.

As the Arab Spring unfolded it was alleged (though yet demonstrated) that Ben Ali and his wife allegedly stole 1.5 tons of gold worth US\$60mio from the central bank before fleeing Tunisia; of the lavish lifestyles of Gaddafi's family members including ownership of expensive real estate and an intertwining of public and personal interests in key state companies and industries; and in the case of Mubarak, common references are made to the "long arm of The Family" Mubarak's corrupt activities continue a long-standing tradition by Kleptocrats who, for example, amassed his own corrupt fortune by improperly taking advantage of business opportunities, but also directed business to

friends and family creating a powerful and loyal elite, much in the same way as Suharto and Marcos had long done before him and as other kleptocrats, such as Saní Abacha, Frederick Chiluba, Joseph Estrada, Saddam Hussein. Other leaders notably corrupt include Arnaldo Aleman, Pavel Lazarenko, Slobodan Milosevic as well as some less senior but still important public officials such as Diepreye Alamieyesiegha, James Ibori, Paulo Maluf. Current serving leaders or recently departed, facing allegations of corruption include Teodoro Obiang and Ali Zardari-Bhutto. Corruption by those holding political office is not limited to countries blighted by endemic corruption, but by all countries with the case of Randy Cunningham in the US a good example.

Money Laundering

As stated earlier, Corruption can involve at least 4 main forms: Petty Corruption, Private Corruption, Organised Corruption and Grand Corruption.

Petty Corruption is where an individual or a business is required to pay a bribe to a public official, often a minor one, for a service, for example in order to obtain a license or other permit or to avoid a penalty, for example a driving violation. The payment will often be made in cash via hand or envelope and spent without touching a financial institution. Whilst this is likely to be the vast majority in aggregate of sums thought to be involved in global corruption, details about actual size are by the very nature of the clandestine arrangements and the lack of the involvement of any responsible intermediary impossible to determine. At the margins, there are questions over whether an act is considered corrupt as opposed to a cultural norm. Take, for example, the long-standing tradition in Asian societies of gift giving. The giving of monetary gifts in red envelopes during holidays or special occasions (e.g. Lei See or HongBao) is an ingrained expected tradition in many Asian societies, there is no corrupt intent or expectation of reciprocity. Similarly, it is difficult to overstate the importance of Guanxi in Chinese society. Guanxi is based on the Confucian hierarchy of relationships, personal connections and favors and is an accepted and legitimate manner of interaction in China. Also take for example the commonplace demand by Irish American waiters in New York Restaurants where a tip is rarely optional.

Private Corruption is where the corruption takes the form of cash or other value passing from the payer to the payee for commercial information, documents or similar, for example, customer lists or other company business secrets. In this form of corruption a public official is usually not involved, unless the company is a state owned business for example.

Organised Corruption exists where organised criminal gangs will pay off a public official to ensure the gangs activities are not hindered or interrupted or that the gang is otherwise protected or granted a form of safe haven, for example to a local police chief who agrees not to investigate or interfere with drug trafficking routes through his area of control. More seriously where the state becomes protector of organised criminal gangs in exchange for money, for example in Panama at the time of President General Manuel Noriega or in Colombia when the Colombian Drug Cartels were at their most powerful and the Cartel of the Suns in Venezuela and Raúl Salinas in Mexico. Beyond Latin-America there is also the case of a terrorist organisation in the form of Al-Qaeda in Afghanistan, when Osama bin Laden paid off the Taliban to remain and be allowed relative freedom and autonomy within Afghanistan prior to the Attacks on America in 2001. Most successful organised crime gangs have managed to buy some level of protection or immunity, particularly in their home market. In the case of organised crime, the funds used to bribe will already be either available in cash or laundered and ready for use.

Grand Corruption is where the most senior figures in a country loot on a “Grand” scale the assets of the country. The funds stolen can originate from many sources including from i) the Central Bank or Sovereign Wealth Fund or similar domestic state owned enterprise ii) from cronies providing “kickbacks” for favors given; iii) by diverting either foreign development aid or loans for investment or foreign State subsidy to ensure continued friendly relations and political support and/or political alignment, or iii) commercial businesses seeking to gain contracts or concessions and to achieve success making funds available, often through intermediaries. The senior public figure may take these assets and funds for themselves, family members and close associates or cronies or they may also direct “funds” to ensure that the senior public figures’ position is maintained or consolidated, for example by directing funds for campaign finance or for bribes to potential opponents or to ensure support. Once the corruption reaches levels of state plunder and renders the State essentially non-viable a state of Kleptocracy has emerged.

Legitimate Companies may also pay bribes to PEPs, particularly Companies regularly winning public contracts in countries with high levels of corruption, where either a bribe is solicited or expected. Industries prone to bribes include Public Works and Construction, Oil and Gas, Mining, Real Estate and Property Development. In each case public officials play an important role in the procurement process and or

the provision of permissions licenses or consents. The amount of the bribe and the seniority or importance of the public official bribed will usually depend upon the size and importance of the underlying contract or transaction. For very large contracts the most senior public figures may be involved, for example, important members of the ruling elite. Examples include major companies such as Siemens, (infrastructure and transport) Statoil (Oil Services), Kellog Brown & Root (Oil Services) and Macmillan Publishing (Public Education)

One Industry which has experienced particular notoriety and claims that bribes are commonplace is the Arms Industry, where governments and leading defence companies trade with each other largely in secrecy and sometimes through Arms Dealers, for example the legendary Adnan Khosoggi. Landmark cases examples include Lockhead Martin, Bofors, BAE Systems and Thomson CSF Thales. A related Industry with Corruption concerns is the military services industry and in particular the operations of Private Military Firms. The use of Intermediaries was and is commonplace and can be a legitimate way of generating business. The use of Intermediaries however, less for their technical expertise and more for their connections to powerful procurement decision makers have often led to suspicions of corruption being raised in connection with Arms Deals but also with other large public sector works contracts. The recent case of Glaxo fined a record US\$3bio for corrupt type practices demonstrates that few industries are without risk.

In order to pay and receive bribes and continue other forms of Corruption, Bribe payers, Intermediaries and Public officials, particularly PEP's have developed elaborate methods to conceal or hide the true nature of the transaction. For example, the use of Intermediaries, complex and opaque structures, the use of cash and the involvement of front companies, family members or close associates. In the Company context, the Bribe is unlikely to be paid directly from the bribing Company to the corrupt PEP, but will often go through one or more Intermediaries after the bribe monies have been segregated from normal company funds or funds come from an already established “slush fund”.

In cases where companies have established a slush fund this has typically been outside the home country of the parent company, most often in an offshore centre or tax haven, with the funds being off-balance sheet or largely unaccounted for, and under the sole signature of a senior employee or even ex employee. These funds are collected perhaps as “rainy day funds” but are used for bribes to third parties, for example

to PEP's for the ultimate gain of the company in its dealings in the country where the PEP can influence decisions in the Company's favour. In order to secure an audience with and agreement from a corrupt PEP, bribe paying Company's have traditionally used trusted intermediaries, with the funds going first to an intermediary or agent acting on the company's behalf as a payment for services or an advanced commission. The amounts paid don't really reflect the services performed indicating that the intermediary will receive something for his involvement but recognising that he will be the conduit through which the bribe is paid, the Company and the PEP therefore seeking to insulate them at least in part from any direct involvement between themselves. These intermediaries will operate accounts and manage the monies to sever the paper trail from the incoming company funds to the transfer of value to the PEP in many different ways, for example using private investment company accounts in different banks and jurisdictions, withdrawals and use of cash. Intermediaries may also employ additional third party Intermediaries or engage with the family members or close associates of the PEP.

Corporate Enforcement Actions

Whilst the SEC has continued to prosecute cases of corruption, since the enactment of the FCPA in 1977, the numbers of cases continues to increase as do penalties for infringements as prosecutions continue to be a high priority area for the SEC. In 2010, the SEC's Enforcement Division created a specialized unit to further enhance its enforcement of the FCPA. Whilst not as active cases have been brought elsewhere too, including in the UK, Germany and France. By taking a closer look at the major cases prosecuted and the penalties levied mostly since 2010,⁸ for major cases resulting in penalties above US\$5mio and before for only the very significant cases, it can be seen that corruption isn't just a problem for emerging markets but is a problem for the most developed countries where household name marque companies, from the US, Germany, Japan, UK, Switzerland, France and Italy amongst them have all paid large fines for paying bribes, and fallen foul of the long arm of both US laws and US muscular enforcement and high tariff penalties with the most recent France's oil giant Total SA paying US\$398mio in connection with bribes to iranians for access to iranian oil and gas fields. Since 2010, fines and disgorgements levied have amounted to more than US\$3bio excluding US\$3bio fine for Glaxo in 2012 which whilst prosecuted under the US False Claims Act also included claims akin to bribery. Going back 5 years and including the Glaxo case penalties are approx US\$8bio and excluding it US\$5bio.

The top 10 cases since 2010 and therefore excluding Siemens (2008 - US\$1.6bio), Kellogg Brown & Root (2009 - US\$579mio) and Glaxo (2012- False Claims Act US\$3bio) (for more details see Part 2, Section 7, Criminal Cases) are as follows:

Top 10 Corporate Corruption Cases since 2010				
No		City	Date	US\$mio
1	<u>Thales</u>	Fr	2011	913
2	<u>BAe</u>	UK	2010	450
3	Total SA	Fr	2013	398
4	ENI	It	2010	365
5	Technip	Fr	2010	338
6	JGC	Jp	2011	218.8
7	Daimler	Ger	2010	185
8	Alcatel 1	Fr	2010	137
9	Alcatel 2	Fr	2011	135.5
10	Magyar Telekom	Hu	2011	95
Total				3.2bio
Source: Author				

Whilst massive illegal financial wealth has been accumulated over the years by corrupt PEPs and others and where much of this accumulated illegal wealth was stored offshore within financial institutions, historically in the PEP's own name or beneficially, and/or conspicuously consumed converting corrupt proceeds into high value goods, more recently the model of transfer and ownership is more likely in the name of others, for example family members or close associates or other “fronts” though effectively controlled by the PEP. Still further of these assets identified, little can be traced back to individual transactions or company initiated bribes.

Gifts and Entertainment

Whilst gifts and entertainment can be a routine part of any business in order to maintain a close relationship with clients, extra care must be taken when the recipient is a public official. Consideration must be given to the nature of the gifts and entertainment to ensure that it is reasonable and proportionate and there is little risk that the acceptance of such hospitality can or be perceived to compromise the official's judgment or integrity.

Counterfeiting & Piracy of Products

"Imitation is the sincerest (form) of flattery"
was first coined by the English writer Charles Caleb Colton in 1820 but it is doubtful that he had counterfeiting or piracy in mind.¹

Harms

The Counterfeiting and Piracy of products is not the victimless crime that much of the public thinks it is when they casually buy a "knock off" designer handbag or a "bootleg" copy of a movie or a music CD. These activities not only infringe the Intellectual Property rights of their owners and creators, stifle innovation and creativity, but may also place consumers at risk. Two of the fastest growing and most profitable counterfeit rackets surrounds counterfeit drugs and machine parts, where inferior products may have life threatening consequences. Because of the profits that can be generated from this illegal activity, organised crime are heavily involved and even terrorist groups have been known to turn to this source of income to fund their operations. Therefore, the purchase of these counterfeited or pirated products to save some money may ultimately result in the indirect funding of a terrorist attack or the support of organised crime activity.

Statistics

The OECD conducted a study on "The Economic Impact of Counterfeiting and Piracy" issuing its initial findings in 2008² and updating these in 2009.³ According to the OECD, international trade in counterfeit and pirated goods amounted to up to US\$250bio in 2007, an increase of more than 25% over the estimated figure reported for 2005 of up to US\$200bio. These figures do not include domestically produced and consumed counterfeit and pirated products, or the significant volume of pirated digital products being distributed through the Internet.

The OECD study estimates that in 2007, counterfeit and pirated goods accounted for a 1.95% share of world trade.

According to Havocscope in 2012 estimated total was US\$691.5bio.⁴ According to the Counterfeiting Intelligence Bureau (CIB) of the International Chamber of Commerce (ICC), counterfeit goods make up 5 to 7% of world trade, which is worth an estimated US\$600bio a year.⁵ Whether the market share is 2% or 7%, the number provides some context for how difficult

it is to detect counterfeit and pirated products given the massive amount of international trade that is conducted.

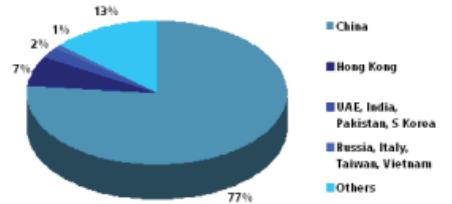
Proceeds from Criminal Counterfeit & Piracy		
Category Type	Est Amount	
1 Counterfeit Drugs	US\$200bio	
2 Counterfeit Electronics	US\$169bio	
3 Software Piracy	US\$63bio	
4 Counterfeit Foods	US\$49bio	
5 Counterfeit Auto Parts	US\$45bio	
6 Counterfeit Toys	US\$34bio	
7 Movie Piracy	US\$58bio	
8 Music Piracy	US\$12.5bio	
9 Counterfeit Shoes	US\$12bio	
10 Counterfeit Clothing	US\$12bio	
11 Cable Piracy	US\$8.5	
12 Video Game Piracy	US\$8.1bio	
13 Counterfeit Sporting Goods	US\$6.5bio	
14 Mobile Entertainment Piracy	US\$3.4bio	
15 Counterfeit Cosmetics	US\$3bio	
16 Counterfeit Aircraft Parts	US\$2bio	
17 Counterfeit Weapons	US\$1.8bio	
18 Counterfeit Watches	US\$1bio	
19 Fake Diplomas & Degrees	US\$1bio	
20 Counterfeit Pesticides	US\$735mio	
21 Book Piracy	US\$600mio	
22 Counterfeit Money	US\$182mio	
23 Counterfeit IDs & Passports	US\$100mio	
24 Counterfeit Purses	US\$70mio	
25 Counterfeit Lighters	US\$42mio	
26 Counterfeit Batteries	US\$23mio	
Estimated Total	US\$691.5bio	

Source: Havocscope⁶

A study released in February 2011 from the Economic Institute Frontier Economics built on the OECD studies and updated their estimates for the value of the international trade in counterfeit and pirated products in 2008 to be between US\$285bio and US\$360bio.⁷ In addition, they developed a methodology to generate an estimate on the domestic production and consumption of such products to be US\$140bio to US\$215bio. Frontier Economics also estimated that in 2008

US\$30 to US\$75bio of digitally pirated products were distributed via the Internet. Lastly, the study projects that the estimated value of the counterfeit and pirated products in these three categories will be between US\$1,220bio and US\$1,770bio by 2015.

Source Countries for Counterfeit Goods



Source: US Customs 2005

In 2012 US Customs reported seized goods of over US\$1.2bio with China (906), Others (183), Hong Kong (156), Singapore (9) and India (7) making up the numbers.

US Customs (2005)⁸ also reported the most popular counterfeited commodities seized as follows: clothes (17%), handbags, wallets and backpacks (16%), cigarettes (10%), footwear (10%), consumer electronics (9%), toys and electronic games (9), computers and hardware (5%), watches and parts (3%), perfumes (3%), pharmaceuticals (2%) and others (15%).

Top 5 Counterfeit Brands

1	Nintendo
2	Nike
3	Adidas
4	Nokia
5	Louis Vuitton

Source: US Customs 2005⁸

According to US Customs, seizures of counterfeit goods increased from approximately 2,000 seizures in 2000, valued at US\$50mio to 13,000 seizures in 2009 valued at US\$250mio.⁹

Definition / Description

To counterfeit means "to make a copy of, usually with the intent to defraud; forge." Piracy,¹⁰ in relation to products, refers to "the unauthorized use or reproduction of copyrighted or patented material."¹¹ Counterfeiting and Piracy are terms that are used to

label a wide spectrum of illegal activities that involve the infringement of Intellectual Property rights such as trademarks, copyrights, patents and design rights. Although the products targeted for Counterfeiting and Piracy used to be mainly luxury goods in order to take advantage of the high value of the imitated product, the scope of product is now wider. Counterfeit designer items such as clothing and watches are still common but one can also find items that could threaten personal health and safety such as pharmaceutical products, illegal drugs, automotive replacement parts, food and drinks. As expected given the wide use of the internet and personal computers, digital piracy of music, movies and software continues to grow. One of the oldest items counterfeited and still imitated is the forgery or counterfeiting of currency, which is its own "Category of Offense" in the FATF Recommendations¹² in addition to the Counterfeiting and Piracy of Products category.

Historical Background / Context

Counterfeiting has a long history, with currency over the years being its principal target. The first monetary coins were made in Lydia, Asia Minor (today Turkey) circa 640 - 630 BC out of electrum, a naturally occurring alloy of gold and silver. Early coins were counterfeited by shaving the edges of the coin (referred to as "clipping") and then using the shavings to make new coins. Currency that consisted primarily of pure gold or silver coins (such as those minted by the early Romans) were counterfeited by mixing various cheaper metals together, casting them as coins and plating them with gold or silver. Those caught, would be punished by death. Images of paper currency printed by Benjamin Franklin in 1777 contain the phrase "To Counterfeit is Death" as it was considered a crime against the state because it was putting the economy in jeopardy. More recently, the english crown created fake continental american dollars during the American Revolutionary War and flooded it into the American economy to the point that the real currency became worthless. Another account of using counterfeiting as a mean of warfare took place during WWII by the Nazis who forced Jewish artists in the Sachsenhausen concentration camp to create counterfeit British pounds and American dollars. Although the quality of the counterfeit bills was very good, the Nazis were unable to execute the plan and the counterfeits were found and destroyed. The Counterfeiting of money continues today and, although the US Secret Service was formed in 1865 expressly to stop the spread of counterfeit US dollars, they are still produced and some high quality counterfeit one hundred-dollar bills have earned the name "Superdollars". The actual creators of these Superdollars are unknown but the US government

believes they are produced by North Korea. While the penalties associated with counterfeiting money are no longer death, they are still more severe than the penalties associated with the Counterfeiting and Piracy of products. In addition, the anti-counterfeiting measures applied to currency are high tech and always evolving. For this reason, although organised criminal gangs are using the latest technology and printing techniques to quickly produce notes of a high quality, most criminals tend to focus their energies on other products where the risk of detection is lower along with the potential penalties. In addition, with the expansion of the internet and digital products in general, the distribution of counterfeited goods and the pirating of digital products in an online environment is quick and easy to do.

Counterfeit products also have a long history, with arguments over the right to copy dating back for example to 600 AD with a dispute in Ireland about a copy of a "Psalter". In the 15th and 16th centuries with the coming of age of printers, laws were developed to control and regulate the output of printed books and materials. The first copyright law, a cornerstone of Intellectual Property rights, goes back to 1709 and the UK "Law for the Encouragement of Learning, by vesting the Copies of Printed Books in the Authors or purchasers of such Copies."¹⁵ Even older is the history associated with trademarks where early versions can be seen in the form of quarry marks on Egyptian structures or "Potters marks" from the Greek and Roman periods. Later, marks or symbols called a "merchants mark" were used increasingly by traders and merchants around the 10th century to establish ownership of goods.

Money Laundering

Despite the size of this market and the undoubtedly massive profits generated by the sale of counterfeited and pirated products, little is available to indicate how the proceeds from these crimes are laundered. Where organised crime is involved, it is assumed that criminal proceeds will be laundered using their existing networks and on the basis of existing available conduits. When we shine a spotlight on the top ten counterfeit / piracy markets, we can gain a better understanding of how large each of these markets is and their impact on society. For a well articulated explanation of the problem and the potential risks and responses for Banks see "Counterfeiting - the US\$650bio Challenge" by Nicholas Kochan.¹⁴

Counterfeit Drugs

According to a 2010 Reuters article, the counterfeit drugs industry is estimated to be worth US\$200bio a year.¹⁵ As the average black market is US\$32.38bio, this makes counterfeit drugs by far the number one

market. A 2012 Reuters article reports that the World Health Organisation (WHO) estimates that around 10% of all drugs around the world are counterfeit.¹⁶ In less developed countries, the percentage of counterfeit drugs in circulation could be as high as 33% (WHO estimated that between 30 to 40% of all drugs and medicine in Pakistan is counterfeit), while in developed countries the rate of fake drugs is less than 1%. This data is supported by a scientific study conducted by the National Institute of Health in the US that found that up to one-third of all malaria drugs taken around the world are counterfeit. The fake drugs and other poor-quality drugs are causing resistance to malaria and failure of treatment. This is a serious issue as around the world as 3.3 billion people are at risk of malaria and it is considered an epidemic in 106 countries. Between 655,000 and 1.2 million people die every year from Malaria according to the BBC News.¹⁷ The head of the Liberia Medicines and Health Products Regulatory Authority stated that up to 60% of the drugs that are on the market in Liberia are counterfeit.¹⁸ The fake drugs enter the country from Guinea on the back of trucks that are not inspected at the border. Many Liberians purchase their medicines from street vendors. Whereas in China, during the two year period from July 2009 to July 2011, police investigated over 42,000 cases of counterfeit drugs and shut down 1,093 illegal websites that were selling fake drugs.¹⁹ Yet despite the life threatening seriousness of the issue (e.g., in Pakistan over 100 patients died at a single hospital due to taking counterfeit heart medications²⁰), the President and CEO of the Pharmaceutical Research and Manufacturers of America stated in March 2012 that the average jail sentence for someone selling counterfeit drugs in the US is three years.²¹

Counterfeit Electronics

2009 Havocscope statistics show that counterfeit electronics are the second largest counterfeit market worth US\$169bio. Meanwhile, in early 2012 it was reported by ZDNet that the number of counterfeit parts entering the supply chain in the global electronics manufacturing industry have quadrupled since 2009.²² In May 2010 it was estimated that 5 to 20% of electronic components in a supply chain is at risk of being counterfeit.²³ 64% of counterfeit electronics sold to consumers in the US takes place in legitimate retail stores, according to Gallop consulting and the US Chamber of Commerce. But this does not just take place in the private sector as the US Navy estimated in early 2012 that up to 15% of all replacement electric circuits and spare parts bought by the entire US Military to be counterfeit.²⁴ The US Senate reported in 2011 that 70% of counterfeit electronics sold to the US Military was traced back to China.²⁵

Software Piracy

In a May 2012 report, search engine company Google reported that it takes down over 1 million links to websites selling counterfeit goods and pirated materials a month.²⁶ The 250,000 links taken down in an individual week in 2012 is more than the total number of links taken down in 2009. The report showed that Microsoft had the most links taken down by Google to enforce their copyrights, with 520,289 links to sites selling pirated software being taken down in the past month.²⁷ This is consistent with a statement in the Wall Street Journal in May 2011 by Microsoft President Steve Ballmer who stated that the company loses 95% of its possible revenue in China due to software piracy.²⁸ According to the US Ambassador to China in December 2011, the sales of legitimate software is higher in Vietnam than in China, despite China having over 15 times the population of Vietnam. Software piracy is believed to be the cause for the low level of sales in China, with an estimated 78% of all software installed on PCs in the country being pirated copies.

The Business Software Alliance reported in its Global Software Piracy Study that US\$63bio was lost to pirated software around the world in 2011.²⁹ The amount lost to software piracy in 2011 was higher than the US\$58bio reported in 2010,³⁰ which was in line with the 2009 statistics reported by Havocscope of US\$58.8bio. Losses in the US due to software piracy in 2011 were US\$9.7bio and the countries of the EU lost US\$14bio. These figures do not include the amount of taxes lost to piracy nor the number of jobs.

Top 10 Countries - 2011 Value of Software Piracy Losses

1	US	US\$9.773bio
2	China	US\$8.902bio
3	Russia	US\$3.227bio
4	India	US\$2.93bio
5	Brazil	US\$2.848bio
6	France	US\$2.754bio
7	Germany	US\$2.265bio
8	Italy	US\$1.945bio
9	UK	US\$1.943bio
10	Japan	US\$1.875bio

Source: Havocscope³¹

Counterfeit Foods

Counterfeit foods around the world creates a US\$49bio a year industry, according to the World Customs Institute in February 2010.³² In the UK alone it is estimated to be a US\$9bio market annually. In April 2009, it was estimated that 10% of the entire food market in the UK was counterfeit.³³ The products globally range from honey to fish and the risks range from just financial to health risks. Some of the more common counterfeited products that seem to just pose financial risks are fake maple syrup, where the expensive maple sugar is substituted in part or entirely with cane sugar, or seafood species that are a different species from the promoted fish name (for example, 77% of fish tested that were labelled for sale as red snapper were actually found to be tilapia, according to a study by the University of North Carolina).³⁴ Luxury food products that emanate from a particular region are often replaced with substandard products but labeled falsely as "French truffles" or "Emmentaler" cheese. One of the most frequently counterfeited products is olive oil. Due to the role of organised crime in Italy, a report found that 80% of the olive oil produced in Italy and stamped with a "Made in Italy" logo was made with cheaper, lower quality oils from other countries. According to research conducted by Food Safety News in 2011, up to 75% of honey that is sold in stores is not real honey since it does not contain pollen. Although consumers may not notice a difference in taste, separate tests found a third of the faux honey imports from Asia were tainted with lead and antibiotics.³⁵ Even more concerning is the production of counterfeit baby formula, which can affect an infant's development since it is not likely to have the recommended levels of protein and other nutrients; in the worst cases, it can lead to death (e.g., in 2004, more than 60 Chinese infants died after ingesting fake formula).³⁶

In late 2011 an operation was coordinated by Europol and Interpol, when they targeted organised crime in a food fraud crackdown. "Operation Opson" (Opson means "food" in ancient Greek) was carried out over a week and spanned 10 countries (Bulgaria, Denmark, France, Hungary, Italy, The Netherlands, Romania, Spain, Turkey and the UK). Authorities confiscated more than 13,000 bottles of substandard olive oil, 30 tons of fake tomato sauce, about 77,000kg of counterfeit cheese, more than 12,000 bottles of substandard wine, five tons of substandard fish and seafood, nearly 30,000 counterfeit candy bars and investigated fake/substandard caviar being sold on the Internet.³⁷ Europol stated that the counterfeit market was a "high profit, low risk activity which undermines legitimate business and puts the safety of consumers at risk". Recent scares and the reaction in the UK

and Europe about horsemeat being used in “value” beef products is indicative of the lack of guarantees in control over and the reliability of some parts of the food chain.

Counterfeit Auto Parts

Counterfeit auto parts in China were estimated to hit US\$45bio in sales in 2011. Out of the total global counterfeit auto parts market, China is responsible for 83% of the counterfeit auto parts that include fake airbags and oil seals as well as spark plugs, brake pads and steering components.³⁸ IP enforcement officials estimate that between 20 to 25% of the auto parts supply market in the United Arab Emirates is made up of counterfeit parts.³⁹ The counterfeit auto parts originate from China, Taiwan, Turkey, Korea and Malaysia and are smuggled and imported into the country. In France, it is estimated that between 5 to 10% of all spare auto parts are counterfeit.⁴⁰ This same figure is attached to the EU where counterfeit auto parts make up between 5 to 10% of all replacement auto parts sold.⁴¹

More troubling are the statistics attached to counterfeit auto parts and lethal automobile accidents. According to a major auto parts supplier quoted in September 2011, up to half of all deaths caused by automobile accidents in Saudi Arabia are caused by the use of counterfeit auto parts, estimated to be a US\$3.4bio industry there. The parts are generally 20 to 30% cheaper to buy when compared to legitimate auto parts. India's Economic Times reported that in 2009, counterfeit auto parts in the country led to 25,400 deaths and over 93,000 injuries.⁴² This is in addition to the loss of legitimate income of US\$1.9bio a year and the cost to the government of another US\$386mio in taxes. The losses are even higher in Indonesia where counterfeit products caused tax losses of up to US\$4.8bio in 2010 with counterfeit automotive parts accounting for almost 17% of the sales.⁴³

Counterfeit Toys

Counterfeit toys is a US\$34bio illegal industry.⁴⁴ Counterfeit toys consisted of 7% of all counterfeit goods seized by EU authorities in 2010.⁴⁵ 98% of the fake toys seized originated from China. Counterfeit toys from China made up 3% of all seizures in FY 2010 by the US Customs and Border Patrol. The value of the seized toys from China was US\$3.7mio. The Anti-Counterfeiting Group estimated in 2011 that counterfeit toys made up to 12% of all toy sales in the UK. This is consistent with estimates provided by the Toy Industries of Europe in 2009 when they said one in ten toys in Europe could be counterfeit. In 2007, the losses to toy makers in Europe were already estimated to be US\$2.1bio annually.⁴⁶

Other country loss estimates were: Brazil US\$31mio, Australia US\$100mio and Mexico US\$1mio.⁴⁷

Movie and Music Piracy

The pirating of movies and music are lucrative black markets valued at US\$58bio and US\$12.5bio, respectively. Pirating is a global problem that continues to grow along with the Internet. Between 45 to 50% of all Internet users in Singapore are believed to access pirated entertainment content, according to the International Federation of the Phonographic Industry (IFPI) in May 2012.⁴⁸ There are around 300,000 incidents of illegally downloading of movies, music and other content each month. Up to 90% of all digital content provided to users on the Internet in Vietnam is pirated.⁴⁹ The content includes music, movies, software and mobile phone apps. According to a poll by Colombia University, 46% of all adults in the US reported pirating copies of a television show, movie or music recording.⁵⁰ 70% of those in the 18 to 29 year old bracket used pirated content, according to the report. According to a 2011 study by the Swiss government, as many as 2.61 million citizens living in Switzerland illegally downloaded pirated content from the internet.⁵¹

Movie piracy creates substantial losses to the film industries in numerous countries. In 2011, movie piracy in Germany created losses of US\$200mio to the film industry. Users in Germany illegally downloaded or viewed unauthorised streams of movies on 185 million occasions. In the same year, the music industry in Germany lost US\$660mio to pirated music.⁵² The Hong Kong Motion Pictures Industry Association (MPIA) estimated in April 2012 that its members lose up to US\$308mio to movie piracy on YouTube. Over the course of three days, the MPIA found over 200 films that were illegally uploaded on to the website.⁵³ The pirated content had over 40mio views on YouTube. The Director General of the Film Academy of the Philippines reported that movie piracy causes losses of US\$95mio to the country's film industry in 2011.⁵⁴

Music piracy is costly to many countries. 99% of digital music downloaded in China is pirated, according to the International Federation of the Phonographic Industry. As of 2012, China has nearly twice as many Internet users as the US, yet its digital music revenue per user is about 1% of the US.⁵⁵ The International Federation of the Phonographic Industry (IFPI) estimated that 28% of Internet users worldwide accessed pirated music online in 2011.⁵⁶

Top 10 Movie Piracy Losses by Country

1	US	US\$25bio
2	China	US\$466mio
3	Mexico	US\$436mio
4	Russia	US\$313mio
5	Bangladesh	US\$180mio
6	UK	US\$165mio
7	Brazil	US\$147mio
8	Poland	US\$118mio
9	Philippines	US\$112mio
10	Argentina	US\$63.4mio

Source: Havocscope⁵⁷

Counterfeit Shoes

Given that the estimated global black market value of counterfeit shoes is US\$12bio, it is no surprise that counterfeit shoes and athletic footwear were the most seized counterfeit items by the US Customs and Border Protection in FY 2010. Fake shoes accounted for 24% of all seizures, with 94% of the shoes originating from China.⁵⁸ This same trend is seen in other countries as it was reported in early 2012 that up to 12 million pairs of counterfeit shoes from China enter Colombia each year.⁵⁹ Mexico reports that up to 200 million pairs of counterfeit shoes enter the country each year as Mexico's crime groups focus their attention on the lucrative pirated goods market.⁶⁰

The counterfeit clothing and counterfeit shoes industry in Australia is estimated to be valued at over US\$658mio.⁶¹ The shoe maker Deckers Outdoor Corp., who makes the popular boot UGGs, reported that nearly 400,000 counterfeit pairs of UGGs were seized around the world in 2010.⁶² In one raid in China, 244,648 pairs of counterfeit UGGs were seized. According to the Korea Intellectual Property Office, 21,454 counterfeit Louis Vuitton products were seized in 2010, followed by 9,118 counterfeit Nike products. Nike shoes are considered to be the most counterfeited brand of shoes in the world.⁶³ One Nike employee told the New York Times that for every one legitimate pair of Nike shoes in the market, a counterfeit pair exists as well.⁶⁴

Counterfeit Clothing

The global black market for counterfeit clothing is estimated to be the same value as the counterfeit shoe market at US\$12bio.⁶⁵ Many of the same criminals that focus on pirating shoes also focus on clothing. As mentioned above, Mexico's crime groups are drawn

to lucrative counterfeiting markets and it is reported that counterfeit clothing in Mexico costs the legitimate clothing industry up to \$9.5bio a year.⁶⁶ France estimates they lose up to \$8.5bio a year to counterfeit goods in general. In 2011, police seized 8.9 million counterfeit goods items in France. Half of the products that were seized within the country were luxury goods items, such as clothes, sunglasses, and cosmetics. Louis Vuitton products were the most counterfeited items seized by authorities in France.⁶⁷

Along with luxury brand items, athletic and sports apparel items are often counterfeited. In 2011, over 60,000 counterfeit clothing and apparel items featuring US college athletic teams were seized by the Collegiate Licensing Company. The value of the counterfeit goods was worth over US\$1mio. Revenue from licensed collegiate athletics generates US\$4.3bio a year for the schools. In addition, there were 4,338 seizures of counterfeit athletic and sports apparel by the US Customs and Border Protection in FY 2010 worth US\$18.7mio. 75% of the clothing came from China.⁶⁸ The Russian Interior Ministry stated that 37% of all clothing sales in Russia are counterfeit clothing. The Ministry stated that most counterfeits are imported into the country, with minimal production of fake goods occurring within the country.

Counterfeit Banknotes

Counterfeiting of banknotes has always been a problem, especially with the introduction of color printers and computer image scanners. The ease of making paper, promotes criminal counterfeiting. Most banknotes are made from cotton paper with a certain weight and sometimes mixed with other textile fibers. Banks and countries have incorporated many types of countermeasures in order to keep the money secure such as embedded holograms, watermarks, special threads, etc. However, with the growth of technology, counterfeiting will remain a serious issue.

The FATF defined Counterfeiting Currency as a predicate offence for money laundering in their 40 Recommendations.⁶⁹ Since 2001, counterfeiting of Euro notes in Greece has been a problem and there were cases in the new member countries as well. In 2003,⁷⁰ there were reportedly 2,411 counterfeiting cases in Greece in which 4,776 counterfeit banknotes were seized. Also in 2003, Polish authorities arrested a gang suspected of creating and trying to introduce a million fake Euros into circulation. The European Central Bank continues to work on ways to combat counterfeiting and money laundering such as considering embedding radio frequency tags into the fibers of higher denomination banknotes since they pose the most risk.⁷¹

Drug Trafficking

[Opium] "prohibition would unleash Organised crime, allow others to step in and fulfill the insatiable demand for narcotics"

William Gladstone , British Prime Minister, 1870

Long considered the most profitable, it is now estimated that illegal drugs are the second most profitable global criminal enterprise after illegal counterfeit and piracy of goods. The Drug Trafficking industry is dominated by organised criminal gangs who are the major players controlling and connecting suppliers via ultimate users.

Harms

The negative consequences of illegal production, trafficking and distribution of illegal drugs is substantial and affects not only individuals who take and abuse drugs but also their families, friends, commercial businesses, governments and societies at large.

The most obvious effects of drug abuse can be seen at the drug user level in ill health, sickness and, ultimately death. Children whose parents and other family members abuse drugs often are physically or emotionally abused and often lack proper immunisations, medical care, dental care and necessities such as food, water and shelter.

The economic impact of drug abuse on businesses whose employees abuse drugs can also be significant, with many drug abusers unable to attain or hold full-time employment and those who do work may put other co-workers at risk. Businesses can also be affected because employees who abuse drugs sometimes steal cash or supplies, equipment and products that can be sold to get money to buy drugs. Moreover, absenteeism, lost productivity and increased use of medical and insurance benefits by employees who abuse drugs can affect a business financially.

The economic consequences of drug abuse severely burden government resources and, ultimately, the taxpayer in connection with both conducting the war on illegal drugs, targeting the transnational drug traffickers and the organised criminal gangs that operate to provide the supply to the domestic criminal gangs that control distribution to the users criminal acts aimed at funding their addictions and providing health and benefits to those in serious medical conditions or need as a result.

In so called Narco States where illegal drug production and/or trafficking is prevalent, the level of crime,

violence and corruption arising out of the drug trade threatens the very productive and functioning existence of these States.

Statistics

According to the UNODC Report issued in October 2011,¹ of the estimated US\$2.1 trillion in crime proceeds generated in 2009, about a fifth, or approx US\$411bio came from illicit drugs, with Cocaine being the highest earner at approx US\$85bio of the more dangerous drugs. The value of the global cocaine market is lower than it was in the mid-1990s, when prices were much higher and the market in the US was strong. In 1995, the global market was worth some US\$165bio, while in 2009, this had been reduced to just over half of that.²

Most Popular Illegal Drugs			Proceeds
1	Cannabis	125-203mio users	US\$140bio
2	Meths	14-57mio users	US\$28bio
3	Ecstasy	11-28mio users	US\$16bio
4	Opioids	12-21mio users	US\$68bio
5	Cocaine	14-20mio users	US\$85bio
	Est Totals	176-329mio users	US\$337bio

Source: UNODC 2009³

While Andean coca farmers earned about US\$1bio, the bulk of the income generated from cocaine was concentrated in North America (US\$35bio), followed by Western and Central Europe (US\$26bio).⁴ Approximately two-thirds of that total may have been laundered in 2009. Global use of cocaine remained largely stable in 2009. UNODC estimates that some 14 to 20 million people used cocaine worldwide.⁵

The global opiate market was valued at US\$68bio in 2009, with heroin consumers contributing US\$61bio of this. Heroin prices vary greatly. Although prices in Afghanistan increased in 2010, one gram costs less than US\$4. In West and Central Europe, users pay some US\$40-100 per gram, in the US and Northern Europe, US\$170-200, and in Australia, the price is as high as US\$230-370. While Afghan farmers only earned some US\$440mio in 2010, organised crime groups in the main countries of consumption reap the largest profits.⁶ Global use of opiates remained largely stable in 2009. UNODC estimates that some 12 to 21 million people used opiates worldwide; some three quarters of them used heroin.⁷

Cannabis remains by far the most widely produced

and consumed illicit substance globally. In 2009, it was estimated by the UN that 125-200 million people used cannabis at least once in that year. Some increases in cannabis use were reported from the Americas, Africa and Asia in 2009, whereas consumption in western Europe and Oceania remained stable or declined.⁸ Despite significant declines in recent years, the largest cocaine market continues to be that of the US, with an estimated consumption equivalent to 36% of global consumption.⁹

UN estimates that some 14 -57 million had used such ATS substances at least once in the past year. For the ecstasy-group for example was estimated at some 11 to 28 million. The predominant substance used varies between and within regions. Amphetamines-group substances dominate in Africa, the Americas and Asia, whereas for Europe and Oceania, the ecstasy-groups prevail. In North America, the two groups are nearly on a par. On aggregate ATS use generally appears stable or increasing, whereas for ecstasy, the trend was stable but decreasing in Asia.¹⁰

Definition / Description

Whilst the term drugs and narcotics are often used interchangeably, in fact drugs like marijuana, cocaine, speed and meth are not "narcotics." The word "narcotic" comes from the Greek word "narkos", meaning sleep. Therefore, technically "narcotics" are drugs that induce sleep, and would apply therefore to drugs such as opium, morphine and heroin. Cocaine and meth are "stimulants", the exact opposite of a "narcotic". They cause people to be more awake and more active, not sleepy.

The Single Convention on Narcotic Drugs of 1961¹¹ consolidated many earlier disparate Treaties and prohibited production and supply of specific drugs, including opium, coca, and derivatives such as morphine, heroin and cocaine and cannabis with a later Treaty the Convention on Psychotropic Substances 1971,¹² adding LSD, Ecstasy, and other psychoactive (Amphetamines and hallucinogens) followed by the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988,¹³ which for the first time introduced provisions against money laundering and other drug-related offenses. Drugs were identified and placed into one of 4 categories or schedules which would determine their perceived dangers to society. The most important perhaps are; Cannabis / Marijuana / Hashish; Amphetamine type stimulants (ATS) and Psychotropic Substances (hallucinogens); Opium / Morphine / Heroin and Cocaine.

Cannabis is both Marijuana (which is a mixture

made of flowers, leaves and small stems of Cannabis) and Hashish, (which is a paste made of the resins from the female flowers and is an intense coffee color). On the physical level, these drugs accelerate the heartbeat, swell the blood vessels and decrease psychomotor coordination. Marijuana and cannabis do not provoke physical dependence, but they can generate psychological dependence and regular use can induce anxiety, tension, insomnia, lack of appetite and temporary irritability.

Amphetamines is the name given to a group of synthetic stimulants¹⁴ which are chemically similar to adrenaline, the hormone used for 'fight or flight' emergencies. This class of drug works on the body's central nervous system and increases its activity. There are three main types: Amphetamines, Benzedrine, more commonly known as "Speed", Dexedrine (Dexedrine or "Dexy's Midnight Runners"); and methamphetamine (Methedrine or "Meth"), the most potent of the three. Amphetamine type stimulants (ATS) can be divided into two main categories: Amphetamines-group (mainly amphetamine and methamphetamine) and ecstasy-group (MDMA and its analogues). Examples of amphetamine substances, include speed, poppers and uppers and of methamphetamine, include crystal meth. Like crack-cocaine, it comes in larger crystals or rocks. When smoked, its effects are comparable to crack in intensity but are much longer lasting and it is highly addictive, since it directly affects the level of dopamine the brain produces.

Opium is made by drying the latex that is found within the opium poppy. It contains about 8 to 10% of morphine and a small amount of codeine. The morphine that is found within the opium is what makes it addictive. It comes in a tar like material. Users commonly smoke it to relieve pain or to get high. Heroin is synthesized from morphine. Heroin is stronger than morphine, and is very addicting. This drug is sold as a powder and in its most pure form, heroin is white, when it is cut (which is most of the time) it is a yellow or light brown color. This drug is most commonly snorted, smoked, or injected.

Cocaine is a powerful drug that comes from the leaves of the coca bush, a plant grown in South America.¹⁵ It's sold as a white powder that is most often snorted (inhaled through the nostrils), but it can also be dissolved in water and injected. Powder cocaine can be chemically changed to create forms of cocaine that can be smoked. These forms, known as "freebase" and "crack", look like crystals or rock.

Historical Background / Context

Man has experimented with drugs for thousands of years. For example, records in China dated to 2737BC show that cannabis was used for medicinal reasons whilst records of opium use predate that date in both Asia and Europe. The use of drugs like morphine (1805), cocaine (1806), heroin (1898) and amphetamines wasn't known until the 19th Century when they were isolated or synthesised by chemists. Latterly LSD was synthesised in 1938 and today a plethora of new compounds emerges regularly. The illegal production, trafficking and distribution of drugs began to flourish in the 20th Century and today is one of the most profitable criminal enterprises in the world generating huge profits for those involved.

Illegal Drugs	Class
Ecstasy; LSD; Heroin; Cocaine; Crack Cocaine; Magic Mushrooms; Amphetamines (if prepared for injection)	A
Amphetamines; Cannabis; Methylphenidate (Ritalin); Pholcodine	B
Tranquillisers; Some painkillers Gamma hydroxybutyrate; Ketamine	C
Source: UK Classes under the Misuse of Drugs Act 1971; Class A penalties are Possession is up to 7 years in prison or an unlimited fine or both and Dealing is up to life in prison or an unlimited fine or both; Class B penalties are Possession is up to 5 years in prison or an unlimited fine or both and Dealing is up to 14 years in prison or an unlimited fine or both; Class C penalties for Possession is up to 2 years in prison or an unlimited fine or both and Dealing is up to 14 years in prison or an unlimited fine or both.	

Opium / Heroin / Morphine

Opium had long been well established, particularly in China and considered a wonder drug. The opium poppy probably reached China through Arab traders who advocated its use for medicinal purposes. In Chinese literature, there are earlier references to its use. The noted Chinese surgeon Hua To of the Three Kingdoms (220-264 A.D.) used opium preparations and Cannabis for his patients to swallow before undergoing major surgery. By the late-1700s the British East India Company controlled the prime Indian poppy growing regions and dominated the Asian opium trade. By 1800, they had a monopoly on opium; controlling supply from mass cultivation in British India and setting prices, this despite the Chinese Imperial court banning its use and importation. In 1839 the Qing Emperor ordered his minister Lin Zexu to address the opium problem which was devastating the Chinese population. An estimated two million Chinese people became addicted

to the drug, with many lives ruined, including the son of the Imperial Emperor, who died after an overdose. Lin petitioned Queen Victoria for help but was ignored. In reaction, the emperor confiscated 20,000 barrels of opium and detained some foreign traders. The British retaliated by attacking the port city of Canton. Thus the First Opium War began. The Chinese were defeated and the Treaty of Nanjing was signed in 1842. The British required that the opium trade be allowed to continue, that the Chinese pay a large settlement, and that the Chinese cede Hong Kong to the British Empire. The Second Opium War began and ended in 1856 over western demands that opium markets be expanded.

The Chinese were again defeated and opium importation to China was legalized and the Chinese were forced to allow it in the Treaty of Tientsin, that substantial quantities of opium poppy to be grown on Chinese soil. Opium smoking was not limited to China, but was sold and smoked initially in opium dens in Southeast Asia, North America and France. It arrived in North America with the large influx of Chinese who came to participate in the California Gold Rush around 1850, disembarking from ships in San Francisco, the city's growing Chinatown became the site of numerous opium dens, run in basements or back rooms, in Chinese run laundries. By the 1870s, San Francisco's opium addiction led in 1878 to the city passing its first anti-opium laws. Opium Dens would also be established in other Cities where Chinese immigrants would establish themselves, for example, in New York. By the early 1900s there were an estimated 250,000 opium addicts in the US, as well as an estimated 200,000 cocaine addicts, supplied in various potions and concoctions derived from Coca leaf imports from Andean countries in South America. Elsewhere in North America, Vancouver in Canada would become an important opium trading centre and in Europe,

French expatriates returning home from their Indochinese colonies established numerous opium dens in France's port cities, particularly Toulon and Marseille. Despite promoting and continued profiteering from the trade of opium to China, the British began to see and respond to the damage drugs could inflict at home and in 1868 passed the Pharmacy Act which restricted the sale of opium to professionals. The profiteering was though on a grand scale and amounted in 1867 to around a fifth of the entire income earned by British India (£7mio). By 1905 the British government now embarrassed by its trade in opium, started to consider changing policy on the trade in opium. The UK and China signed a Treaty declaring the opium trade illegal in 1908, though the Treaty would take years to implement. Mounting international concern,

particularly over the spread and dangerous effects from opium which had reached worldwide epidemic proportions, led in 1909 the US, to initiate a series of intergovernmental meetings, first in Shanghai, and then at the Hague in the Netherlands in 1911, which resulted in the signing of the International Opium Conventions 1912 (Hague Convention) where signatory states pledged to curb the production, distribution and consumption of opium, morphine, heroin and cocaine, and to restrict the use of these materials to 'legitimate medical purposes.' Ratification and implementation was effectively suspended by the commencement of World War 1 but eventually the end of the War would bring about the opportunity in 1919, when Article 295 of the Treaty of Versailles incorporated the Hague Convention, and committed Versailles signatories at last to the implementation of its anti-drug measures. In the meantime some Countries, for example the US in 1914 had passed laws implementing the 1912 Hague Convention terms (the Harrison Act). Britain passed the Dangerous Drugs Act in 1920, which made it illegal to possess opiates without a doctor's prescription. Cannabis would be added in 1928. With demand still high for drugs like opium, and traditional suppliers no longer willing to supply, the market became dominated by illegal operators. In fact the Great British Prime Minister, William Gladstone (who liked to take a drop of opium in tea or coffee before making speeches) had predicted this very outcome in the event of prohibition in a debate in the British Parliament in 1870. He told Parliament that prohibition would unleash Organised Crime in the region and allow others to step in and fulfill the insatiable demand for narcotics. In 1925, a statistical control system of all transactions concerning narcotics which was to be supervised by a Permanent Central Opium Board was introduced as part of The International Opium Convention (the "Geneva Convention").

Amphetamines Type Stimulants (ATS)

Increased demand for Amphetamines and hallucinogens started in the US, in the 1960s centred first around San Francisco, where a century before, opium established itself in America as the 1960s ushered in a counterculture that led to social change. Out of this counter-culture, emerged a worldwide youth culture, in which drug use assumed a prominent and often integral role. The counter-culture movement took hold in Western Europe, with London, Amsterdam, Paris and West Berlin rivaling San Francisco and New York as counter-culture centres. One manifestation of this was the French general strike that took place in Paris in May 1968, which nearly toppled the French government. Another was the German Student Movement of the 1960s. In Central Europe, young people adopted the

song "San Francisco" as an anthem for freedom, and it was widely played during Czechoslovakia's "Prague Spring", a premature attempt to break away from Soviet repression. The rise in popularity of amphetamines coincided with the rise in popularity of a relatively new substance, LSD, and at its height in 1967 as the so called "Summer of Love" saw hippie culture reach its height. Lysergic acid diethylamide better known as LSD or acid, was known for its psychological psychedelic effects. LSD was first synthesized and accidentally ingested by Albert Hofmann in 1938, later being Introduced by Sandoz Laboratories, in Switzerland. Albert Hoffman would eventually establish himself and his company as one of the leading Pharma Conglomerates, under the name Hoffmann Laroche. In the 1950s, officials at the US Central Intelligence Agency (CIA) thought the drug might be applicable to mind control and chemical warfare; it certainly had mind altering qualities which were experimented with by many including pop stars such as the Beatles in the 1960s. The increased recreational use of drugs by youth culture in the Western world during the 1960s led to a political firestorm that resulted in a political backlash. In 1971, US president Richard Nixon initiated a policy calling it the War On Drugs, declaring drug use to be 'Public Enemy Number One'. The stance adopted by the Nixon regime took US drug policy to an even more aggressive level, fully committing the country for the foreseeable future to a law-enforcement solution to the problems associated with drugs. US policy has yet to emerge from this project, and continues to deploy its influence, economic, diplomatic and military in discouraging other UN countries from adopting any alternative approaches. In 1988, Ecstasy (MDMA) fueled a so called rave culture in the UK and beyond when ravers experienced a second Summer of Love. The youth movement rejected individualistic values based on the consumption of alcohol and sex, instead being 'Loved-up' on E, young ravers in their thousands danced away the night at outdoor festivals.

Cocaine

As recently as the late 1970s, many experts and public health officials wrongly believed that cocaine was a relatively benign substance and primarily of interest as a "recreational" drug. This would change within 5 years, with supply and dosage increasing. The production of coca in South America expanded from a cottage industry of small groups of subsistence farmers into a major agricultural business that was financed by organised families or "cartels." The manufacture and trafficking of cocaine became a multibillion dollar industry, with profit margins high enough that governments and entire legal systems became corrupted by the influx of cocaine industry money. Supplies of

cocaine into the US increased exponentially. During the early to mid-1980s, according to DEA reports, the estimated amounts of cocaine entering the US doubled and tripled year after year. These supplies of cocaine made the drug available in purer form and at a more affordable cost to consumers. The drug traffickers then realized that cocaine could be manipulated into so called "crack cocaine" which caused an American epidemic as the "crack" was then sold as small rocks in a mass retail operation, with rocks being sold at a cost of US\$10 to US\$20. This new product was extremely addictive and inexpensive and was readily available to a much wider user base. By late-1985 and early-1986, the retailing of crack cocaine had swept through most urban centres of the US. The introduction of crack into urban communities produced devastating consequences. Health-related problems, rapidly escalating rates of addiction, and an extraordinary wave of street crime and property crime swept through most major American cities. In many areas, American Street Gangs were central to the distribution and sales of crack. Warfare between American Street Gangs battling over turf resulted in many fatalities among gang members as well as innocent bystanders in the community. As drug-related crime escalated dramatically, legal penalties for sales of cocaine and crack were increased, and US jails and prisons rapidly filled with crack users, dealers, distributors, and those involved in the violence associated with the crack trade. In the late 1990s and into the first decade of the twenty first century, three-quarters of the world's annual yield of cocaine was produced in Colombia, both from cocaine base imported from Peru and Bolivia, and from locally grown coca and the Cocaine trade was dominated by the Colombian Cali and Medellin Cartels, both became notorious and the target of Colombian and US Law Enforcement.

In 1995 US President Clinton issued Executive Order 12978, "Blocking Assets and Prohibiting Transactions with Significant Narcotics Traffickers," under authority of the International Emergency Economic Powers Act¹⁶ and called upon the Treasury to target Colombian drug cartels using financial sanctions. Under this authority, OFAC launched the Specially Designated Narcotics Traffickers ("SDNT") programme. The objectives of the SDNT programme were said "to isolate and incapacitate the businesses and agents of the Colombian drug cartels by publicly exposing them, freezing their assets, and denying them access to the financial system and to the benefits of trade and transactions involving US businesses and individuals. The SDNT list referred to "527 companies and 815 individuals involved in the ownership or management of the 21 Colombian drug cartel leaders' business empires. The

businesses named as SDNTs range across industries and included drugstore chains, a supermarket chain, pharmaceutical laboratories, airlines, a medical clinic, hotels, restaurant service companies, radio stations, sports teams, communications companies, construction firms, real estate firms, investment and financial companies, consulting companies, offshore firms, horse breeding farms and other agricultural businesses, mining operations, maritime agencies, and a department store." Nevertheless and despite Herculean efforts to fight the mainly US led war on drugs and the expenditure of billions upon billions of dollars, victory remains elusive. With increased attention and prices on their heads, the Leaders in Cali, Gilberto and Miguel Rodriguez Orejuela, and in Medellin, Pablo Escobar would be brought eventually to justice, the former being captured, extradited and imprisoned in the US in 2006 and the latter through a bullet which would end his life in a shootout with Colombian Police in 1993. Until then and for over 20 years, these individuals and the Cartels would become the world's biggest and most profitable criminal narcotic organisations. In 1989, for example, Forbes magazine declared Pablo Escobar as the seventh richest man in the world, with an estimated personal fortune of US\$25bio. Whilst Cocaine production in Colombia remains high, Cocaine production dominates the Bolivian economy producing about 30% of the world's cocaine supply.¹⁷ With drugs accounting for a large proportion its whole economy dwarfing other legitimate sectors. Money Laundering is a serious problem in Bolivia with few effective controls. Peru is in a similar position but with a larger coca crop and a burgeoning poppy crop.

The 10 Drug Traffickers (last 50 years)		Net Worth
1	Pablo Escobar	US\$30bio
2	Amado Carrillo Fuentes	US\$25bio
3	Dawood Ibrahim Kaskar	US\$6.7bio
4	The Ochoa Brothers	US\$6bio
5	Khun Sa	US\$5bio
6	Jose Gonzalo Rodriguez Gacha	US\$5bio
7	The Orejuela Brothers	US\$3bio
8	Carlos Lehder	US\$2.7bio
9	Griselda Blanco	US\$2bio
10	Joaquin Loera Guzman	US\$1bio

Source: Celebrity/Net Worth

Money Laundering

Whilst the profits to be made in connection with the drug production, trafficking, and distribution of illegal drugs are huge, it is the drug traffickers who make most of the profits, ensuring the drugs get to market via established but evolving transit routes. Still whilst they are the single biggest group, the drug traffickers have to share the profits with producers and street gangs who largely sell to end users and with others involved in the process.

Cannabis

Cannabis remains by far the most widely produced and consumed illicit substance globally. Cannabis herb cultivation is widely dispersed as it is mostly produced for domestic or regional Markets. However, the countries most often identified as sources of cannabis resin are Morocco, Afghanistan, Lebanon, Nepal and India.¹⁸

Heroin

Heroin enters Europe primarily by two major land routes linking Afghanistan to the huge markets of Western Europe and the Russian Federation. The long-standing 'Former Yugoslav or Balkan or Southern route traverses the Islamic Republic of Iran (often via Pakistan - Iran currently has the largest prevalence of opiate consumption in its population globally and receives the bulk of Afghanistan's opium production, in part for consumption and for onward export, but also Iran also accounts for 84% of total global opiate seizures).¹⁹ Turkey, Greece, Albania and Bulgaria across South-East Europe to the Western European market, with an annual market value of some US\$20bio. Much of the Heroin is controlled in its passage via the "Southern Route" by the Turkish and Albanian Mafias. The northern route runs mainly through Tajikistan and Kyrgyzstan (or Uzbekistan or Turkmenistan) to Kazakhstan and into the Russian Federation, Russia (and is sometimes colloquially referred to as the 'silk route') with an annual market value estimated at approx US\$5bio per year. Much of the Heroin is controlled in its passage via the "Northern Route" passing through Central Asia for Russia and Western Europe by the Russian Mafia.

Whilst many have accused Triad gangs of involvement in cross border drug trafficking. A US Justice Department funded report published in 2007 into drug trafficking between Myanmar and China noted that the Hong Kong drug trade is primarily dominated by loosely connected individuals of Chinese descent BUT there is no evidence to suggest any direct link between regional drug trafficking and Hong Kong / Chinese Triads. This study provides first hand data

depicting how Chinese drug traffickers operate in the Golden Triangle and surrounding countries.²⁰ Law enforcement sources in the region seemed to agree that Chinese nationals are almost always involved in major drug raids. According to the Australian Federal Police noted most major drug manufacturing and trafficking activities in Southeast Asia and elsewhere in the Pacific region are linked to Chinese criminals.

Unregulated and internal money transfer systems also play a major role in Money Laundering related to Heroin Trafficking. In and around Afghanistan for example and because of the lack of a modern banking sector, financial transactions are handled mainly by the hawala system.

In Faizabad, for example, during certain times of the year it is believed that close to 100% of the liquidity of the hawala system in this province is derived from drugs, whereas in Herat, the Northern Alliance stronghold, it is believed that only 30% of the hawala market's overall transaction volume is directly linked to drugs. The southern region (Helmand and Kandahar provinces) is also a key centre for money laundering in Afghanistan (about 60% of the funds are drug related and 80- 90% of the hawala dealers in Kandahar [the Taliban stronghold] and Helmand are involved in money transfers related to narcotics). Helmand has emerged as a key facilitator of the opium trade, both between provinces and exports, while overall estimates of the local hawala markets' drug-related component of a similar order of magnitude to those in Kandahar. This finding adds weight to the notion that the major trading centres in these two neighbouring provinces should be treated as essentially one market. Bearing this in mind, the study calculated that Helmand could account for roughly US\$800mio of Afghanistan's drug-related hawala business and that Herat is the second largest contributor, with in the range of US\$300-500mio of drug money laundered annually. Furthermore, Dubai appears to be a central clearing house for international hawala activities. In addition, various cities in Pakistan, notably Peshawar, Quetta, and Karachi, are major transaction centres. It appears that even in the case of drug shipments to Iran, payments for them come into Afghanistan from Pakistan. The hawala system has been key to the deepening and widening of the "informal economy" in Afghanistan, where there is anonymity and the opportunity to launder money.

Cocaine

The US State Department estimates that 90% of cocaine entering the US transits through Mexico.²¹ Cocaine is moved from Colombia and other Andean countries (particularly Bolivia and Peru) and shipped in

numerous ways with most controlled by the Colombian & Mexican Drug Cartels. These include principally by land through Central America into and through Mexico or by air and transported to staging sites in northern Mexico. The cocaine is then broken down into smaller loads for smuggling across the US–Mexico border. The primary cocaine importation points in the US are in Arizona, southern California, southern Florida, and Texas. Typically, land vehicles are driven across the US-Mexico border. Sixty five percent of cocaine enters the US through Mexico, and the vast majority of the rest enters through South Florida, via smuggling routes throughout the Caribbean, in particular via the Bahamas Island chain. The traffickers use a variety of smuggling techniques to transfer their drugs to US markets. These include the commercial shipment of tonnes of cocaine through the port of Miami as well as airdrops in the Bahamian Islands or off the coast of Puerto Rico, mid-ocean boat-to-boat transfers and then fast speed boats to the Miami area. Lately even submarines are thought to be used. Unmanned subs are towed underwater so no radar profile and if towing boat approached it can ditch instantly so no evidence if boarded. Transponders allow later recovery on some. Cocaine is also carried in small, concealed quantities across the border by couriers known as “mules” (or “mulas”), who cross a border either legally, for example, through a port or airport, or illegally elsewhere. The drugs may be strapped to the waist or legs or hidden in bags, or hidden in the body. If the mule gets through without being caught, the gangs will reap most of the profits. If he or she is caught however, gangs will sever all links and the mule will usually stand trial for trafficking alone.

In December 2010 the government of Spain remarked that Mexican Cartels have multiplied their operations in that country, becoming the main entry point of cocaine into Europe. The Mexican Army crackdown has driven some cartels to seek a safer location for their operations across the border in Guatemala, attracted by corruption, weak policing and its position on the overland smuggling route.²² The smugglers pick up drugs from small planes that land at private airstrips hidden in the Guatemalan jungle. The cargo is then moved up through Mexico to the US border. Guatemala has also arrested dozens of drug suspects and torched huge cannabis and poppy fields, but is struggling. In February 2009, Los Zetas Cartel threatened to kill the President of Guatemala, Alvaro Colom. On 1 March 2010, Guatemala's chief of national police and the country's top anti-drugs official have been arrested over alleged links to drug trafficking. A report from the Brookings Institution warns that, without proactive, timely efforts, the violence will spread throughout the

Central American region. Mexican and Colombian Drug Cartels have established bases in West African nations. They are reportedly working closely with local criminal gangs to carve out a staging area for access to the lucrative European market. The Colombian and Mexican Cartels have discovered that it is much easier to smuggle large loads into West Africa and then break that up into smaller shipments to Europe - mostly Spain, the UK and France. Higher demand for cocaine in Western Europe in addition to North American interdiction campaigns has led to dramatically increased trafficking in the region: nearly 50% of all non-US bound cocaine, or about 13% of all global flows, is now smuggled through West Africa.²³

Black Market Peso Exchange

The Colombian Drug Cartels have developed and employed the Black Market Peso Exchange. For details about how this works and other laundering techniques see Part 1, Section 1, Smuggling; Cash Smuggling below and Part 1, Section 2, Sub-section 2, Money Services Businesses below.

Amphetamine Type Stimulants (ATS)

Africa is a region of concern with regard to the trafficking of ATS. Trafficking of methamphetamine from Africa was reported first at the end of 2008 and reports have continued since. West Africa, in particular, is emerging as a new source of methamphetamine for illicit markets in East Asia, with couriers transiting Europe, West Asia or East Africa. Precursor chemicals are also frequently trans-shipped through the region. In India, the first clandestine ATS manufacture operation was detected in May 2003. Since then, several additional facilities have been uncovered. Attempts at illicit ATS manufacture has also been reported from Bangladesh and Sri Lanka. South Asia has become one of the main regions used to obtain ephedrine and pseudoephedrine for the illicit manufacture of methamphetamine. India is one of the world's largest manufacturers of precursor chemicals and Bangladesh also has a growing chemical industry. Amphetamine, methamphetamine and ecstasy have been regularly seized in South Asia over the past five years.²⁴

For more details about how Drug Traffickers operating as organised crime gangs and how they approach money laundering see Organised Crime below in this Part 1, Section 1 and for details of the leading Organised Crime /Drug Trafficking organisations see Part 2, Section 5, Criminals and Terrorists below.

Environmental Crime

*“Environmental degradation, over-population, refugees, narcotics, world crime movements and organised crime are worldwide problems that don't stop at a nation's borders”
Warren Christopher, 63rd US Secretary of State for under President Clinton¹*

Harms

Environmental crime is a serious and growing international problem, with criminals violating national and international laws put in place to protect the environment. These criminals are polluting the air, water and land. They are pushing commercially valuable wildlife species closer to extinction and they are significantly impacting the biological integrity of the planet. Once perceived as ‘victimless’ and low on the priority list, such crimes are increasingly the focus of government action. The impacts affect all of society. For example, illegal logging contributes to deforestation. It deprives forest communities of vital livelihoods, causes ecological problems like flooding, and is a major contributor to climate change. Up to one-fifth of greenhouse gas emissions stem from deforestation.² Illicit trade in ODS like the refrigerant chemicals chlorofluorocarbons (CFCs), contributes to a thinning ozone layer, which causes human health problems like skin cancer and cataracts.

Statistics

Environmental crime is currently one of the most profitable forms of criminal activity and it is no surprise that organised criminal groups are attracted to its high profit margins. Estimating the scale of environmental crime is problematic but Interpol estimates that global wildlife crime is worth billions of dollars a year.³ Interpol also reported that illegal logging was US\$30-100bio a year.⁴ The figure is much higher than the US\$15bio reported by the World Bank earlier with illegal logging destroying land the size of a football field every 2 seconds.⁵ The UN Environment Programmes reported that between 15-30% of the world's timber supply is provided by illegal logging activities.⁶

According to Europol, the trafficking of endangered species is worth US\$32bio with Europe the prime destination.⁷ For more on wildlife smuggling and poaching see Smuggling below.

As far as chlorofluorocarbons (CFCs), and ozone depleting Substances (ODS) are concerned, the 1990s saw around 38,000 tons traded illegally every year, equivalent to 20% of global trade in CFCs and worth US\$500mio.⁸ Since then, in 2006 for example still up

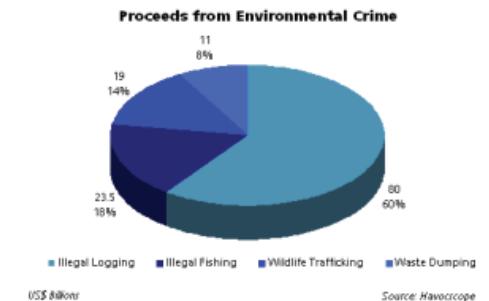
to 14,000 ton of CFCs were smuggled into developing countries.⁹

Illegal Fishing activities around the world account for 19% of the world's catches, according to the EU.¹⁰ The EU criticises Belize, Cambodia, Fiji, Guinea, Panama, Sri Lanka, Togo and Vanuatu for not doing enough to stop the activity.

According to the Federation of American Scientists,¹² the US Government estimates that local and international crime syndicates worldwide earn US\$22-31bio annually from hazardous waste dumping, smuggling proscribed hazardous materials, and exploiting and trafficking protected natural resources and that the tremendous costs for legally disposing of pollutants and dangerous chemicals have created new illicit business opportunities for criminal organisations, who earn US\$10-12bio per year for dumping trash and hazardous waste materials.

According to Havoscope the illegal fishing problem is upward of US\$23.5bio¹¹ with estimates for illegal logging at US\$30bio, for wildlife trafficking at US\$19bio and waste dumping at US\$11bio, amounting in aggregate to US\$83.5bio.

For Oil & Gas see Smuggling below.



Definition / Description

Environmental crimes can be broadly defined as illegal acts which directly harm the environment. They include: illegal trade in wildlife; smuggling of ozone depleting substances (ODS); illicit trade in hazardous waste; illegal, unregulated, and unreported fishing; and illegal logging and the associated trade in stolen timber, trafficking and use of illegal pesticides and the illegal diversion of rivers. They can also cover negligent acts which result in oil and gas spills or chemical and toxin releases or even nuclear accidents. Environmental crimes by their very nature are trans-boundary and involve

cross-border criminal syndicates. A tiger skin or an ivory tusk passes through many hands from the poaching site to the final buyer. A tree cut down illegally can travel around the world from the forest via the factory to be sold on the market as a finished wood product. In the era of global free trade, the ease of communication and movement of goods and money facilitate the operations of groups involved in environmental crime.

Environmental criminals, including those associated with organised crime, regularly cause permanent and extensive damage to ecosystems, which may result in serious human health problems. The incentives to carry out environmental crimes are financial, coupled with a perception, on the part of criminals, that they are unlikely to be caught and face severe penalties. Examples of environmental crimes which have become more common and lucrative are the trade of collectible species and illegal disposal of waste in an effort to avoid legitimate disposal costs, which results in an unfair competitive advantage for the criminals over legitimate, law-abiding businesses.

The focus on protecting the Environment has gradually increased across the World with more than 250 international and regional environmental agreements being developed in the thirty years since the first landmark UN Conference on the Human Environment in Stockholm in 1972. The US was one of the strongest proponents' of action, itself passing strong Environmental Protection Laws and began to enforce these.

Selected Major Fines for Environmental Crimes			
No	Name	When	US\$
1	BP - so far	2010/12	5.25bio
2	Exxon Valdez	1989	532.5mio
3	Union Carbide	1989	470mio
4	Walmart	2013	110mio
5	Amoco Cadiz	1978	85mio
6	Cunard Line	1996	23.5mio
7	Carnival Cruises	2002	18mio
8	Royal Caribbean	1999	18mio
9	Probo Koala	2006	€1mio

Source: Author (whilst fines can be large, the clean up costs can dwarf the fines, for example the Exxon Valdez cost more than US\$2bio)

In 1982, the US Environmental Protection Agency's (EPA) Office of Criminal Enforcement was established leading to an increase in prosecution of environmental crimes. Cases that demonstrate both public anger and a response by the authorities included action against Donald Distler, who was prosecuted for his contamination of the Louisville, Kentucky sewer system and sentenced

to two years in prison and fined US\$50,000, and the Kepone contamination episode in Virginia which resulted in fines of over US\$13mio. In 1992, The Convention on Biological Diversity was adopted under the auspices of the UN Environment Programme. Its aims are the conservation of biological diversity, the sustainable use of biological resources, and the fair and equitable use of benefits arising from the use of genetic resources. Interpol since 1992 has also taken a lead in identifying emerging patterns and trends in the field of environmental crime enforcement. For more details see for example Operation Worthy in Part 2 Section 7 below.

Historical Background / Context

The Industrial Revolution began in Britain in the 1700s, and spread to the rest of the world, at first Europe and the US and later elsewhere. The use of machinery and factories led to mass production, which in turn led to the development of numerous environmental hazards and damage, which would only be seen clearly years later. The use of factories and mass production has led to a depletion of certain natural resources, leaving the environment permanently damaged. One example of this depletion is deforestation, which is the clearing of forest trees for use in production. When the trees are cleared, the wildlife in the forest also becomes uprooted.

Deforestation - Over 50% of the world's animals and plants come from Brazil's rainforests, which also create 40% of the world's oxygen. Ranchers, farmers and loggers are responsible for the majority of rainforest destruction, mowing down over 10,000 acres of forest each year. Deforestation releases green house gases, which are readily contributing to climate change on a global level. As oxygen is crucial to the ability of all species to survive, rainforest destruction presents a threat of epic magnitude to every being on the planet. The lack of trees is only compounded by the problem of carbon emissions. Whereas forests would help emit oxygen and refresh the levels of healthy gases in the air, factories are emitting poisonous emissions and eliminating the oxygen source. The pollution that has resulted from factories involves not only airborne emissions but land and water pollution as well. The primary issue resulting from pollution and carbon emissions is that of global warming. As the temperature rises, the glaciers are melting and oceans are rising. More animal species are becoming endangered or extinct as a result of global warming. Another issue is Mountaintop Removal Mining.

Mountaintop Removal Mining (MTR) - MTR is a method used by mining companies to more cheaply extract coal by avoiding mining underground; instead Companies remove the top soil and trees or whatever is above the coal seam and then using explosives blast away at the earth until the coal seam is finally unearthed. The coal can then easily be removed by diggers and taken away by trucks. Once the coal is extracted the seam should be filled in and the area landscaped in such a way as to resemble the land as before. Despite good intentions, Environmentalists are critical of such

techniques which inevitably cause lasting damage to the environment. Overfishing remains a problem too.

Overfishing - this has had many detrimental effects on the environment, from changing the ecosystem to polluting the waters that so many creatures depend on for life. The climate of our world depends on the health of the ocean for stability, and overfishing has caused the populations of all fish to decrease over the last twenty years.

CFCs/ODs - Chlorofluorocarbons (CFCs) and other halogenated ozone depleting substances (OD's) are mainly responsible for man-made chemical ozone depletion. The ozone layer prevents most harmful ultraviolet light (UV light) from passing through the Earth's atmosphere and its depletion is suspected of causing a variety of biological consequences such as increases in skin cancer, cataracts, damage to plants, and reduction of plankton populations in the oceans which are at the base of the oceans' food chain. CFCs were invented by Thomas Midgley, Jr. in the 1920s. They were used in air conditioning and cooling units, as aerosol spray propellants and in many cleaning processes. Whilst the full extent of the damage that CFCs have caused to the ozone layer is not known, as this takes decades to fully see the results, the situation has improved following co-ordinated action after a 1976 report by the US National Academy of Sciences concluding that credible scientific evidence supported the ozone depletion hypothesis.

In 1985, 20 nations, including most of the major CFC producers, signed the Vienna Convention for the Protection of the Ozone Layer, which established a framework for negotiating international regulations on ozone-depleting substances. That same year, the discovery of the Antarctic ozone hole was announced, causing a revival in public attention to the issue. In 1987, representatives from 43 nations signed the Montreal Protocol. Still it would take until a 1992 meeting in Copenhagen, that a final phase out date was agreed being 1996. To some extent, CFCs have been replaced by the less damaging hydrochlorofluorocarbons (HCFCs), although concerns remain regarding HCFCs also. In some applications, hydrofluorocarbons (HFCs) have been used to replace CFCs. HFCs, which contain no chlorine or bromine, do not contribute at all to ozone depletion although they are potent greenhouse gases. More recently, policy experts have linked ozone protection efforts to climate protection efforts.

The upside of the Industrial Revolution has certainly been the mass production of food for an increasing world population and the massive increase in living standards and life expectancy. While the Industrial Revolution is the cause of positive change for the industrial world, there is no question that it has severely damaged the environment. The depletion of natural resources, the carbon emissions, pollution and human health problems, the effect on animals, the countryside, and many traditional peoples way of life's is the price paid so far.

The growth in the so called BRIC Countries, (Brazil, Russia, India and China) and others not so large but numerous have only exacerbated the problem. Some of the most devastating environmental disasters have occurred in the last 50 years, not only causing serious damage to the environment but also to human life and human health. Although many environmental disasters can be blamed on nature itself, hurricanes, tornadoes and earthquakes, there are still a few catastrophes that without doubt remain the fault of our species alone.

The most important of which include toxic chemical releases in Seveso, Italy, the so called Love Canal, US, Bhopal, in India, the Baia Mare cyanide spill, Romania and from the freighter Probo Koala; mining disasters, including the Spanish waste water spill in Aznalcollar, Spain and the Tennessee coal ash spill as well as damage from mountain top removal;

Notable Major Environmental Disasters	
1976	Seveso, Italy - Dioxin
1978	Love Canal, US - Toxins
1984	Union Carbide, Bhopal, India - Toxins
1986	Chernobyl, Ukraine - Nuclear
1986	European BSE Crisis - Livestock
1988	Great Pacific Garbage Patch - Trash
1991	Exxon Valdez, Alaska, US - Oil
1991	Kuwaiti Oil Fires - Oil
2006	Probo Koala - Waste
2010	BP Deepwater Horizon Gulf Mexico - Oil

Source: Author

Further there have been nuclear incidents in Three Mile Island in the US and Chernobyl, Ukraine; damage to the oceans from massive overfishing and waste dumping creating the Great Garbage Patch in the Pacific Ocean and the almost extinction of the Aral Sea from diverting rivers upstream; damage to animals and livestock for example the Bovine Spongiform Encephalopathy (BSE) Crises, in Europe; illegal and sustained deforestation particularly in Brazil but also for example in Indonesia from which regular Indonesian forest fires result and last but not least serious numerous oil and gas spills, including from the Amoco Cadiz, the Piper Alpha explosion in the North Sea; the Exxon Valdez sinking off Alaska; the Kuwaiti Oil Fires at the start of the Gulf War oil spills in the Niger Delta and the BP Deep-water Horizon spill in the Gulf of Mexico.

Money Laundering

The major motive for most environmental crime is financial gain. Environmental crime is not restricted

by borders and often involves criminals who engage in other crime types such as Murder, Corruption, Forgery and Fraud. A significant proportion of both wildlife and pollution crime is carried out by Organised Crime Groups, drawn by the relative low risks and high profit nature of these types of crime. The same routes used to smuggle wildlife across countries and continents are often used for smuggling Arms, Drugs and Humans and as for these crimes much of the proceeds are generated in Cash and the laundering of the funds are usually “cleaned” through Organised Crime laundering networks. Corruption presents a major hurdle to successfully combatting Environmental Crime. Corrupt Public Officials, trying to “cash in” have been involved in signing off on import and export certificates, facilitating the transport of illicit goods and ‘turning a blind eye’ as and when required. Far more serious, and yet just as common, is the complicit, long-term involvement of individuals from the police, army, government and intergovernmental organisations. Protected by familiar bureaucracies, weak legislation and poor enforcement, corrupt officials can thrive through environmental crime.

Whilst there have many sectors that have damaged the environment, none are more publicly followed by the media than the Oil & Gas sector, not in many cases for wilful or criminal acts but for negligent or unsafe practices which have led to some of the worlds most damaging environmental consequences. Beyond Oil & Gas, Waste Disposal and Waste Smuggling are an increasing cause also of concern, alongside Chemical and Shipping spills, damage to the Oceans and Seas and Livestock affecting the food chain.

Oil and Gas

Amoco Cadiz: In 1978 the Liberian super tanker Amoco Cadiz under charter by Amoco Oil Corporation lost control of its steering mechanism and soon became grounded off Brittany in France. The ship broke in two releasing 230,000 tons of crude oil, polluting approximately 300 kilometres of coastline, destroying fisheries, oysters and seaweed beds as well as many beaches and local Breton communities. Amoco was ultimately required to pay US\$85mio for the costs of the spill.

Piper Alpha: In 1988 an explosion occurred on the oil and gas production platform Piper Alpha in the North Sea, killing 167 out of 240 on board. The Cullen Enquiry was set up to establish the cause of the disaster, pointing to a leakage of natural gas building up beneath the platform, because of faulty maintenance work on a pump and a related safety valve, resulting in the ignition

of secondary oil fires and the melting of upstream gas pipelines. Piper Alpha's operator, Occidental, was found guilty of having inadequate maintenance procedures.

Exxon Valdez: In 1989 the American oil tanker Exxon Valdez ran aground in Prince William Sound in Alaska trying to avoid some small icebergs present in the region. The collision with the reef caused an oil discharge of 32 million gallons polluting 1900 kms of coastline. The oil spill killed approximately 250,000 sea birds, 2,800 sea otters, 250 bald eagles and possibly 22 killer whales. Exxon Mobil, the owner of the Exxon Valdez, was originally fined with punitive damages of around US\$5bio, equal to a single years profit for Exxon at that time. However, following appeals it finally agreed to pay a criminal fine of US\$25mio and a civil fine of US\$900mio and had the punitive damages reduced to US\$507.5mio. Exxon is thought to have spent more than US\$2bio for the clean-up operation. Ironically, official NOAA (National Oceanic and Atmospheric Administration) investigations have shown that most of the damage from the oil spill was caused by the cleaning operation following the disaster. It is claimed that pressure-washing was responsible for killing most of the marine life. In order to pay the fine, Exxon is thought to have obtained a loan from JP Morgan & Co, who themselves, had created the first modern credit default swap, so that Morgan's could protect themselves against the risk of Exxon's credit default.¹³

Kuwait Oil Fires: In 1990 Iraqi forces invaded Kuwait, leading to the 1991 Gulf War, which ejected Iraqi forces from Kuwait but left the regime is Saddam Hussein intact. In January 1991 ahead of the start of the Gulf War, Iraqi forces committed two environmental disasters. The first was a major oil spill 16 kms off the shore of Kuwait by dumping oil from several tankers and opening the valves of an offshore terminal. The second was the setting fire to 650 oil wells in Kuwait. Approximately one million tons of crude oil was discharged as a result, making this the largest oil spill in human history. It took until November 1991 before the last oil fire well was extinguished. The poisoned waters killed 20,000 seabirds and caused severe damage to local marine flora and fauna. The fires caused soot and toxic fumes to enter the atmosphere, having great effects on the health of the local population.

Niger Delta: In Nigeria, Shell is regularly criticized for Oil spillages into the Niger Delta, though the Company blames criminals and terrorists for much of the environmental damage. Since 2006 Shell has faced regular attacks by criminals and terrorists, who target pipelines, kidnap petroleum company workers and fight with government troops. The spillages occurred largely through intentional damage at a wellhead and

a bombing of a pipeline. Shell reported that 51 of its employees and contractors were kidnapped for ransom in 2009, compared with 11 in 2008.

BP Deep-water Horizon: The 2010 BP Deepwater Horizon, Oil Spill in the Gulf of Mexico, is the most recent and perhaps most significant oil spill in history when nearly 5 billion gallons of crude oil was discharged. A final report was released on the spill in January 2011. It blamed BP, Halliburton and Transocean for making a series of cost cutting decisions, as well as system issues putting safety at risk. It concluded that the spill therefore was not the fault of any rogue individual or company but by systemic company failures. BP agreed to pay an initial fine of US\$4.5bio in 2012 and admitted it was guilty of manslaughter. Additional civil fines of up to US\$17bio are still possible. The total bill for monies paid out or set aside so far is US\$42bio with estimates that the final cost may reach US\$60bio. Adding further fire to BP's fuel, the company settled in 2012 with the SEC, paying US\$525mio for incorrect statements made about the size of the flow of oil misleading investors.

BP had already pleaded guilty to a felony for failing to immediately report illegal dumping of hazardous waste by a contractor in 2000, the biggest-ever oil spill on Alaska's North Slope in 2006, and a 2009 pipeline rupture near the Lisburne Production Centre also in Alaska. In addition, “Occupational Safety and Health Administration (OSHA) statistics show BP posted 760 ‘egregious, wilful’ safety violations – while Sunoco and Conoco-Phillips each had eight, CITGO had two and Exxon had one comparable citation.” In two separate disasters prior to the Deepwater Horizon, 30 BP workers were killed and hundreds have been seriously injured. BP pleaded guilty to a federal misdemeanor in the 2006 oil spill, put on three years probation and had to pay US\$20mio in fines and penalties, plus US\$25mio to settle a civil lawsuit brought by the federal government. BP is not alone in the Oil Industry as having damaged the Environment.

Waste Disposal

Probo Koala: Beyond the Oil Industry, the transportation of hazardous materials is a major concern. The case of Trafigura and the Probo Koala is interesting. Trafigura was found guilty in a Dutch court for illegally delivering hazardous waste to Amsterdam on the freighter Probo Koala whilst concealing its true nature and then exporting this toxic waste to Ivory Coast, in 2006, which according to the Ivory Coast government led to the deaths of 16 people with thousands suffering health problems connected to

the waste. Trafigura was fined €1mio by the Dutch authorities and paid €33mio to the victims of the illegal dumping.

Chemicals

Baia Mare: The 2000 Baia Mare cyanide spill was a leak of cyanide near Baia Mare, Romania, into the Someş River by the gold mining company Aurul, a joint-venture of the Australian company Esmeralda Exploration and the Romanian government.

The polluted waters eventually reached the Tisza and then the Danube, killing large numbers of fish in Hungary and Yugoslavia. The spill has been called the worst environmental disaster in Europe since the Chernobyl disaster. The spill contaminated the drinking supplies of over 2.5 million Hungarians. Wildlife was particularly affected on the Tisza: on a stretch, virtually all living things were killed, and further south, in the Serbian section, 80% of the aquatic life was killed. Large quantities of fish died due to the toxicity of cyanide in the waters of the rivers, affecting 62 species of fish, of which 20 are protected species. For details on the toxic releases in [Seveso Italy](#) and [Bhopal India](#) see Part 2, Section 7 below.

Oceans and Seas

Whilst our oceans and the fish and seabirds that they support have been damaged by numerous oil and gas spills, water and waste dumping, as can be seen from the Cases above, two further examples demonstrate the damage being inflicted. These are the cases of the Great Garbage Patch and the case of the Aral Sea.

Great Garbage Patch: The patch exists in the North Pacific in a slowly moving, clockwise spiral of currents. The currents have brought together so much trash, 90% of it plastic, creating the largest landfill in the world. The UN Environment Programme estimated in 2006 that every square mile of ocean hosts 46,000 pieces of floating plastic.¹⁴ In some areas, the amount of plastic outweighs the amount of plankton by a ratio of six to one. According to Greenpeace more than 200 billion pounds of plastic the world produces each year, about 10% ends up in the ocean and 70% of that eventually sinks, damaging life on the ocean floor.¹⁵ The rest floats; much of it ends up in gyres and the massive garbage patches that form there.

Two large masses of ever-accumulating trash, known as the Western and Eastern Pacific Garbage Patches are known as the Great Pacific Garbage Patch. An Eastern Garbage Patch floats between Hawaii and California;

scientists estimate its size as two times bigger than Texas and a Western Garbage Patch formed east of Japan and west of Hawaii.

Aral Sea: The Aral Sea was a vibrant ecosystem in central Asia until massive diversion of the inflowing Amu Dar'ya and Syr Dar'ya rivers were allowed to provide irrigation water for local farmers. These diversions dramatically reduced the river inflows, causing the Aral Sea to shrink by more than 50%, to lose two-thirds of its volume, to wipe out fishing and to greatly increase its salinity affecting drinking water. Downstream, the salt pollution is decreasing the available agriculture area, destroying pastures, and creating a shortage of forage for domestic animals. The number of domestic animals in the region has become so low that the government has issued a decree to reduce the slaughter of animals for food. At the current rate of decline the sea is estimated to disappear by 2020. Diseases like anaemia, cancer and tuberculosis, and the presence of allergies, are on the rise. The incidence of typhoid fever, viral hepatitis, tuberculosis and throat cancer is three times the national average in some areas. Recent measures have been taken to change this disastrous state, through the International Fund for Saving the Aral Sea (UNEP, GRID Arendal, IFAS, 1997). If all measures are adhered to, a substantial recovery might be achieved within 20 years, although it is doubtful that the Aral Sea will ever be restored to the conditions that existed before the large-scale diversion of its inflowing rivers.

Livestock

BSE Crises: Bovine spongiform encephalopathy (BSE), commonly known as mad cow disease, made the headlines when the EU banned exports of British beef from 1996 until 2006. In the UK, the country worst but not only affected, more than 180,000 cattle were infected and 4.4 million slaughtered during the eradication programme. An inquiry into BSE concluded that it was caused by cattle, which are normally herbivores, being fed the remains of other cattle in the form of meat and bone meal (MBM), which caused the infectious agent to spread. The increased concern of BSE was that the disease could be transmitted to humans, where it is known as Creutzfeldt-Jakob disease which killed 166 people in the UK, and 44 elsewhere. Between 460,000 and 482,000 BSE-infected animals had entered the human food chain before controls on high-risk offal were introduced in 1989.

Shipping

Whilst fines for water discharging over the years

have been numerous and fines depending upon the seriousness of the case ranging from thousands of dollars to millions of dollars¹⁶ with the two largest being those levied below, the largest fine, for environmental damage by shipping was levied in 1996 against the Cunard Line for the actions of Royal Viking Sun, which struck a coral reef at the mouth of the Gulf of Aqaba, causing substantial damage to the reef. The company was fined US\$23.5mio. Royal Caribbean Cruises pled guilty in 1999 paying US\$18mio to settle US charges for fleet wide practices of discharging oil-contaminated waste, regularly and routinely discharging without a permit wastewater contaminated by pollutants through its ships' water systems, and making false material statements to the US Coast Guard. These practices for example occurred around Alaska, Miami, New York City, Los Angeles, Puerto Rico and the US Virgin Islands. Carnival Corporation pled guilty in 2002 to discharging oily waste into the sea from their bilges by improperly using pollution prevention equipment. In addition, it falsified its books in order to conceal its practices and as a result was fined US\$18mio.

Retailing

Walmart: One of the world's biggest retailers admitted in 2013 violating criminal and civil laws to protect water quality and agreed to pay more than US\$110mio in fines. Walmart employees regularly discarded hazardous materials such as pesticides, solvents, detergents, paints, aerosols and cleaners into municipal trash bins and into local sewers.

Nuclear

Whilst Nuclear has long been considered one of the safest and most reliable forms of power generation, not least because the consequences in case of major incident are potentially catastrophic, incidents have nevertheless occurred which have caused death and injury to life and harm to the environment. As well as the fall out from these incidents, the potential damage to the environment and the costs from used nuclear materials are increasingly causing concern.

Whilst the events at Three Mile Island¹⁷ in Pennsylvania in the US could be brought under control and a melt down avoided, the incident at Chernobyl near Kiev in the Ukraine was more serious. More recently the events following the tsunami in Japan, at the Fukushima nuclear power plant in Japan, whilst not man made, still serve to illustrate the potential dangers when nuclear power is compromised.

Extortion

"To count upon his virtue and use it as an instrument of torture, to practice blackmail with the victim's generosity as sole means of extortion, to accept the gift of a man's good will and turn it into a tool for the giver's destruction."
Ayn Rand, Novelist, Philosopher¹

From the schoolchild who gives up his lunch money to the bully for fear of getting picked on to the Hollywood depiction of wise guys "shaking down" a business owner for a monthly payment, Extortion shows up in our world in many different forms. The common element is that no one wants to be coerced into doing something they do not want to do or to live in fear because they had the guts to say no. Standing up to an Extorter is a brave thing but it is more difficult to do if the demand is coming from a Public Official or a member of an organised crime gang. Extortion is a word you often hear paired with the term organised crime. In fact, when one reads about the activities associated with specific organised criminal gangs, extortion is generally on the list. Many organisations that are designated as terrorist groups now function in the same manner as organised crime gangs in terms of how they finance their operations and Extortion is a common technique employed.

Harms

Besides the immediate fear of losing your life or a loved one's life and the stress that accompanies living with that fear, another harm of extortion comes from distorting trade as well as from the destruction of property that can often occur in tandem. Where extortion inflates the cost of business, it also distorts the playing field, protecting companies with connections from competition and thereby sustaining inefficient companies.

Statistics

Statistics related to extortion are very hard to come by and are most often combined with kidnapping or kidnapping for ransom statistics for obvious reasons. As with any criminal activity, it is very hard to get numbers surrounding the activity since the goal is not to get detected. This becomes even more difficult with Extortion since victims rarely report the crime to the police due to fear.

According to Havocscope, a crime statistics organisation estimates that, for example, in Mexico, up to 80% of all extortion attempts in Mexico go unreported. Of the reported cases of extortion, the number of cases has tripled between 2004 and 2011.²

Definition / Description

Extortion is the criminal activity by which any person (or entity) who, with a view to securing an unlawful gain (such as money, property or services) for himself or for another, coerces another person (or entity) to do something by using violence, or a threat with serious detrimental consequences (for example, financial loss, reputational damage, etc.).

Refraining from doing harm is often referred to as "protection." There is no global definition so each jurisdiction has its own that may emphasize certain points.

For instance, under US federal law, the definition makes it clear that Extortion can be committed with or without the use of force and with or without the use of a weapon. It further explains that it may be committed across a computer system, phone, by mail or in using any instrument of "interstate commerce" and that the person who sent the message must have "willingly" and "knowingly" done it.

The FATF define Extortion as a predicate offence for money laundering in their 40 Recommendations. Extortion is a form of Corruption and in its worst cases may also involve kidnapping and hostage taking or murder. Extortion is sometimes coupled with the word bribery but there is a distinct difference since bribery is the offering of something of value in order to get a certain wish met and Extortion is a threat of violence or other bad things if a certain wish is not met (obtaining something of value).

Further the FATF states in their Terrorist Financing Typologies Report that extortion may be used by supporters of terrorist and paramilitary groups to exploit their presence within expatriate or diaspora communities to raise funds through extortion. The criminals tax the diaspora on their earnings and savings. These extortions are targeted against their own communities where there is a high level of fear of retribution should anyone inform the authorities.

Historical Background / Context

Throughout history there are instances where different groups have used Extortion against others or even examples of countries extorting money from other countries. Of course the countries requesting "tributes" or special taxes for various reasons may not have viewed it as a form of extortion. In ancient China, the tribute system was formed as a means of trade regulation and it also allowed China to maintain authority over neighboring countries. The neighboring countries paid tributes (generally in the form of large sums of money)

to show their respect for China and gain the right to trade with them. In return, these countries maintained their own sovereignty and were not conquered by China.

Another early use of extortion that also involved the paying of tributes in order to avoid being attacked was utilised by the Barbary Pirates, a name derived from the “berber” people of North Africa, and a region similar to the Maghreb today, and home to Pirates and Slave traders from the 17th Century. Until 1776, American ships were effectively protected from the Barbary Pirates due to British treaties with the North African states. Morocco, after earlier recognising the US's independence, became the first Barbary power to seize an American vessel in 1784. Although the US secured peace treaties, it still was required to pay tribute for protection from attack. Payments in ransom and tribute to the Barbary states amounted to 20% of US government annual expenditures in 1800. The Barbary Wars in 1801 and 1815 finally led to the end of the payment of tributes by the US.³

Money Laundering

Extortion ranges from minor forms like the lone guy in the street who “offers” for a fee to watch your car in a bad neighborhood (so that it doesn't get stolen or damaged), to the demand for payment from a foreign government so that an oil rig is not dynamited. The Italian Mafia has long been associated with Extortion as are most organised crime gangs today. The Italian Mafia focuses on public sector extortion, the Japanese Yakuza on corporate extortion (or “Sōkaiya”), the Triads operate mainly by extortion from large Chinese ex-pat communities.

Terrorist Groups realise there is money to be gained through Extortion and it is one of the main sources of funds for ETA. The “revolutionary tax” is demanded by ETA from business owners in Spain, particularly in the Basque Country, under threats to them and their families. The Provisional IRA started demanding “protection” money from pub owners and other local shopkeepers and businessmen in the early 1970s in a very overt and threatening manner. Today, the extortion still continues but now the approach to a new business is made by a legitimate security company as opposed to a bunch of thugs waving weapons. In Russia and the other former Soviet states, there are around 6,000 mafia groups whose basic business is extortion. It is not surprising that former Ukrainian Prime Minister Pavlo Lazarenko was sentenced in 2004 to nine years in prison by a US court for extortion, among other crimes. Another leader that utilised Extortion during his reign was Francois Duvalier (known as Papa Doc) who was

the president of Haiti From 1957 to 1971. His son Bebe or Baby Doc Duvalier continued the practice when he succeeded his father.

The Japanese Yakuza frequently engage in a uniquely Japanese form of extortion, known as Sōkaiya. In essence, this is a specialized form of protection racket. Instead of harassing small businesses, the Yakuza harasses a stockholders' meeting of a larger corporation. They simply scare the ordinary stockholder with the presence of Yakuza operatives, who obtain the right to attend the meeting by a small purchase of stock. They also engage in simple blackmail, obtaining incriminating or embarrassing information about a company's practices or leaders. Once the Yakuza gain a foothold in these companies, they will work for them to protect the company from having such internal scandals exposed to the public.

Some companies still include payoffs as part of their annual budget, for examples see Part 2, Section 7, Criminal Cases, Glico-Morinaga and Kiyoshi Takayama. While the Yakuza use a more unique form of Extortion than other organised crime and terrorist gangs, the list of groups utilizing Extortion techniques is long. In one of its training manuals, Al-Qaeda refers to the “carrying out [of] threats (extortion) against other regimes if they do not give willingly”. In this case “one or two assassinations should be carried out so that the regime would realize that we are serious about our threats”. The same applies to international companies such as “pharmaceutical companies, airline companies, insurance companies and petroleum companies, big industrial companies and meat companies, fruit companies”. More examples using the technique of targeting the diaspora of a certain nation or group include the Tamil Tigers and Al Shabaab.

Extortion that involves a direct monetary payment as opposed to the performance of a service or the transfer of physical property is much easier to detect and would involve your classic monitoring for money laundering in terms of third party payments and the ascertainment of the purpose of the payment and the relationship between the third parties. When the third parties involved are Politically Exposed Persons (PEP) or connected with a sensitive industry or country, extra scrutiny is applied to the transactions.

Since Extortion is often coupled with other crimes and is often utilised by organised crime, the focus tends not to be solely on Extortion but rather on the organisation. Therefore, the money laundering methods may be similar as for other types of organised crime activities.

Forgery

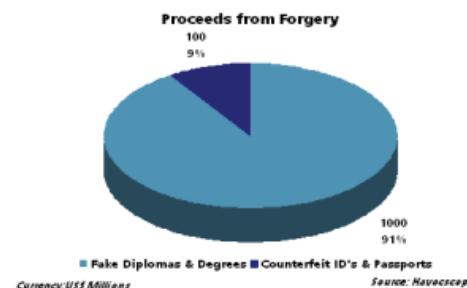
*“You utter a vow or forge a signature and you may find yourself bound for life to a monastery, a woman or prison.”
Bronislaw Malinowski, Anthropologist¹*

Harms

Forgers are used by both organised crime gangs and terrorist groups to further their criminal activities. For example, Riduan Isamuddin (aka Hambali), an Indonesian terrorist and the mastermind of the 2002 Bali attacks and alleged leader of Al-Qaeda-linked Southeast Asia terror group Jemaah Islamiyah, acquired forged passports which were then used by members of Jemaah Islamiyah to travel to Indonesia. The 2002 Bali bombings led to the deaths of 202 people.

Statistics

The nature of Forgery itself makes the accumulation of Statistics in order to size the crime very difficult. It is also the case that much of the systematic forgery, for example in relation to identification documents, occurs underground and the better the forgery the harder to detect. Evidence suggests that the forgery of Higher Education Certificates are probably the most prevalent and profitable areas, followed by forged identification documents including passports. According to Havoscope, estimates for proceeds from fake diplomas and degrees are US\$1bio and for fake IDs and passports US\$100mio.



Definition / Description

Forgery is the creation of a false written document, the alteration of a genuine document, or a signature falsely created or altered, with knowledge of the false nature and the intent to defraud. The Instruments of forgery may include bills of exchange, promissory notes, cheques, bonds, receipts, orders for money or goods, mortgages, deeds, public records, certificates of education or achievement, account ledgers, and certain

kinds of tickets or passes for transportation or events. Counterfeiting is often associated with forgery but relates more to physical goods as opposed to documents, though it does include currency.

Some areas of forgery are niche crimes and auxiliary to other crimes that generate more financial profit. Passport forgery is usually conducted by small workshops, and the method is often that they alter stolen passports. However, it is not easy to buy a forged passport since they are usually sold within criminal networks where relationships of mutual trust have already been established. These networks are global and cross the ethnic boundaries of different groups of organised crime. There are some areas of forgery that operate on an industrial scale and sell to anybody who is willing to pay. In these areas very sizeable profits are generated, for example, in the production of fake IDs for Americans under 21 years old who want to drink alcohol, and in the creation of forged educational and professional credentials. A high quality of fake US driver's licenses can be ordered for between US\$75 and US\$300 from merchants in China that produce and ship them in hidden compartments in shoes and other items. In the US city of Chicago alone, customs intercepted more than 1,700 fake IDs in the first half of 2011. US customs has estimated that ID forgers from China who are targeting this US market earn millions or even tens of millions of US\$ annually.² The forgery of educational credentials may be even more profitable and together with forged pay slips, these credentials can be used for example in fraudulent loan applications.

Historical Background / Context

The law of forgery may have originated with an early Roman law around 80 B.C. that prohibited falsification of documents describing the passing on of land to heirs. The precise scope of what was considered forgery at common law is not universally agreed upon, but a statute passed in the time of Queen Elizabeth I in the 17th century prohibited forgery of publicly recorded, officially sealed documents with the intent to affect the title to land, as well as the knowing use of such documents as evidence in court. In the first major expansion of the law's coverage, a 1726 decision declared that a false endorsement on an unsealed private document was indictable both under the Elizabethan statute and at common law. Writing only half a century later, William Blackstone was able to declare, after referring to several contemporary statutes, that “there is now hardly a case possible to be conceived wherein forgery, that tends to defraud, whether in the name of a real or fictitious person, is not made a capital crime”. Blackstone defined common law forgery, which he also called crimen falsi, as “the fraudulent making or altering

of a writing to the prejudice of another man's right." Pillory, fines, and imprisonment were the penalties in those rare cases that were not subject to capital punishment.

Perhaps the most famous case of forgery in the twentieth century took place in 1983 with the "discovery" of the Hitler diaries. The diaries supposedly contained passages written by German dictator Adolf Hitler between 1932 and 1945. Gerd Heinemann, a German reporter for Stern magazine, claimed the writings as genuine and sold them. He had obtained them from Konrad Kujau, a dealer in military memorabilia and documents. Newsweek and Paris Match, along with other media, paid more than US\$5mio for the documents. Major news sources around the world quickly published detailing the historical information that the diaries allegedly contained. Investigative experts from around the world later conducted forensic examinations on the diaries and found the documents to be forged. Kujau then admitted forging the diaries, and news sources immediately retracted their coverage. Both Kujau and Heinemann were sentenced to four and a half years in a German prison. Another famous forger of the 20th Century was Elmyr de Hory who successfully forged works of art, though died still a pauper.

In the US, the Mormon Bible forgeries resulted in more extreme consequences. Beginning in the early 1980s, Mark Hofmann, a disillusioned Salt Lake City Mormon and part-time dealer in historical documents, forged documents of major importance to Mormon history. He sold most of the creations to the Mormon Church and to others interested in Mormon religious history. Hofmann reaped hundreds of thousands of dollars from his fraud. His boldest forgery, the White Salamander letter, cast doubt on the credibility of the Mormon Church's founder, Joseph Smith. In this letter, Hofmann portrayed Smith as a dabbler in folk magic and the occult, which greatly distressed the Mormon community. When individuals within Hofmann's ring of buyers raised doubts about the authenticity of one of his later creations, Hofmann murdered one buyer and the spouse of another before their suspicions became public. Hofmann was arrested and charged with murder and fraud. The prosecution agreed to negotiate the charges to avoid an embarrassing trial for the Mormon Church. Hofmann pleaded guilty to Murder. In January 1988, the Utah Board of Pardons sentenced Hofmann to life in prison without parole.

The World Customs Union (WCU) helps promote international strategic cooperation in the fight against forged travel documents. In particular since the September 11th terrorist attacks, for national security

reasons, combating the forgery of travel documents are very high on the agenda of the US and other governments. Security features of passports and visa documents have vastly improved, and so has the security around the storage of blank documents. Nonetheless, there exist criminal syndicates that attempt to forge travel documents on a massive scale. Thailand is known as the capital for passport forgery since the act of forgery is considered a petty crime. After the September 11th attacks and after the Bali bombings in 2002, the Thai government has cracked down on forgery. In May 2008 Thai authorities seized 21,000 fake passports and in December 2009 Thai authorities arrested five people who allegedly produced and smuggled more than 300 fake EU passports.³

A recent conviction in the UK of a gang known as the History Men serves to illustrate how criminals profit from preparing forged identification and other documents. For more details see Part 2, Section 7, Criminal Cases.

Aside from the forging of travel documents, historical documents, and other documents one cannot ignore two of the most prevalent forged documents used by fraudsters, namely those used to perpetrate Prime Bank Guarantee and forged Promissory Note Frauds. Although promissory notes are legitimate investments, those that are marketed broadly to individual investors (especially the elderly) and entities including municipalities, charitable associations and others often turn out to be scams. The fraudster almost always presents a forged document promising guaranteed massive returns with little or no risk. Another tell-tale sign is the mention of secrecy and/or the claim that the investment opportunity is by invitation only or reserved for sophisticated investors, giving the fraud a claim of exclusivity. Similar tactics are used for Prime Bank Guarantee Frauds. For more details see Part 1, Section 1, Fraud below.

Money Laundering

Since most transactions involving forged identifying documents or travel documents are paid in cash little data is available that shows how proceeds of these forgeries are laundered. Where organised crime is involved it is assumed that criminal proceeds will be laundered using their existing networks and on the basis of existing available conduits. Forgers that operate on an industrial scale, like those in Thailand and in China creating fake identifying documents, may have similar networks for laundering criminal proceeds as the organised criminal networks. However, those who operate in small cells or alone will most likely use their criminal proceeds for personal use.

Fraud incl Tax Fraud & Cybercrime

"Only when the tide goes out do you discover who's been swimming naked"

Warren Buffett - legendary US Investor & Philanthropist¹

The types of fraudulent schemes appear limitless and ever-changing and affect every type of financial activity across the entire world. They do, however, share a certain commonality in that the fraudster usually induces the victim to depart with their property, often in the form of money, by false representations of material facts. As the Warren Buffett quote above suggests, in good times, many abuses, including Frauds remain hidden, but in challenging economic periods many Frauds become apparent as investors look for the return of their monies or property.

Harms

While usually carried out without actual or threatened violence, Fraud undermines the integrity of both Commerce and Markets, generating significant criminal proceeds for the criminals involved. With the evolution of the Internet, fraudsters can now reach millions of potential victims quickly and at minimal cost, thus coining the term Internet Fraud.

Fraudulent schemes perpetrated against individuals or groups, particularly vulnerable groups like seniors, or particular markets can ultimately have a devastating impact on those defrauded and the viability and operation of the markets affected. Individuals who fall victim to fraud can experience physical, psychological, financial and social damage. The impact of fraud can also be detrimental for corporate victims. Small/medium sized companies are sometimes unable to recover from the financial or reputational damage caused. Large multinational organisations can feel the effects through the increased cost of doing business. Where the government is victimised, it may pass on its losses to the public such as increased taxes or reduction in services.

Statistics

According to the Association of Certified Fraud Examiners in the US fraud costs US organisations more than US\$400bio each year, with the median loss caused by men, who commit 75% of the offenses, being US\$185,000; the median loss caused by women is US\$48,000. Losses caused by managers are four times bigger than those caused by employees. The median losses caused by executives are 16 times the size of those caused by employees.² Fraud schemes can be very difficult to detect. The median length of the schemes from inception to discovery was 18 months. The median recovery among victim organisations was only 20% of the original loss. Almost 40% of victims recovered nothing at all. Most occupational fraudsters are first time offenders. Less than 8% of the fraudsters had a previous conviction for a fraud-related offense. The most common occupational frauds in small businesses involved: employees fraudulently writing company cheques, skimming revenues or processing fraudulent invoices.

The UK National Fraud Authority estimates that in 2010, Fraud cost the UK £38.4bio.³ There are many types of Financial Fraud schemes. It has been estimated that securities fraud totals approximately US\$40bio per year in the US. In the UK, the FSA estimates the cost of Boiler Room Fraud to be £200mio per year.⁴

Based on the US and UK figures for fraud losses, total global losses if following similar patterns would amount to approx US\$2.75 trillion or between US\$2.3-3 trillion.

"Frauds by country"

According to the UN which ranked countries in order of size per GDP versus the amount of Fraud found that the leader board was dominated by countries with large successful economies, with Germany topping the list, followed by the US and then the UK.⁵

Frauds by Country			
1	Germany	11	Italy
2	US	12	Japan
3	UK	13	India
4	France	14	Sweden
5	Korea, South	15	Austria
6	Poland	16	Czech Republic
7	Canada	17	Hungary
8	Russia	18	Netherlands
9	Mexico	19	New Zealand
10	South Africa	20	Finland

Source: "Frauds by country", The Eighth UN Survey on Crime Trends and the Operations of Criminal Justice Systems (2002) (UNODC)

According to US General Keith Alexander, Director of the National Security Agency and Commander of US Cyber Command, cyber attacks and cyber crime amount to "the greatest transfer of wealth in history". Putting figures on cyber crime and losses due to cyber attacks is difficult though two figures are often quoted, the first from Symantec, a software security group that intellectual property theft costs US companies US\$250bio a year and a figure from McAfee, a rival firm, that cyber crime globally costs US\$1 trillion a year. General Alexander has used in his remarks the former figure and President Obama has mentioned the latter though little direct evidence has been put forward

to back up these figures.

McAfee has recently revised their US\$1bio estimate, following a study by the Center for Strategic and International Studies (CSIS) and sponsored by McAfee, which concluded cybercrime caused a loss to the global economy of between US\$100bio and US\$500bio, with the estimated loss due to cybercrime and cyber espionage for the US economy of US\$100bio.⁶

Definition / Description

Fraud is essentially theft carried out by deceptive means and usually without the use or threat of violence but by manipulative techniques or practices to acquire monies for personal gain. Fraud is not always premeditated, though it often is. It can instead result from losses being incurred and a desire to cover up either the losses themselves or to make up gains by fraudulent activity, with or without personal gain.

Although most countries have their own laws that make Fraud a criminal offense, the severity of the offense and punishment for those who are found guilty vary greatly depending on the country and the type of Fraud committed. The FATF Recommendations designates Fraud as a predicate offence and FATF has published guidance on specific types of fraud, such as their 2007 paper "Laundering the Proceeds of VAT Carousel Fraud".⁷ In their recent update of the FATF Recommendations, FATF added tax crimes to the list of predicate offences for money laundering. This addition will bring the proceeds of Tax Fraud within the scope of the powers and authorities used to investigate money laundering - which are typically far more extensive and intrusive than those used to investigate "ordinary" crime.

Historical Background / Context

The history of fraud goes back millennia and has probably been around since the very early days of commerce. One of the first recorded examples of attempted Fraud involved a Greek merchant named Hegestratos in 300 BC who took out a large insurance policy known as bottomry. Hegestratos borrowed money and agreeing to pay it back with interest when the cargo he was shipping - in this case corn - was delivered. The lender as security for the loan was entitled to acquire the boat and its cargo in case of default. Hegestratos' plan was to sink his empty boat, having secretly off-loaded his corn, thus defrauding the lender of his money, the corn or the boat, but his plan came unstuck when he drowned whilst sinking his boat.

Under Roman law, for example Law 265 stated "if a herdsman to whose care cattle or sheep had been entrusted, be guilty of fraud..." he could be punished by a forfeit of ten times the value of the fraud or in some cases, his life should "be solemnly forfeited," or ended. Nevertheless fraudulent practices were commonplace and rather than punishing offenders the Latin and legal maxim, "Caveat Emptor," or let the Buyer Beware became the watchword largely governing commercial

transactions before more effective legal arrangements began to be developed in English Common Law in the 16th Century onwards..

Fraudulent schemes appear limitless in variety and fraudsters come in all shapes and sizes. Some of the largest recorded have led to great historical events, for example fraudulent activity materially contributed to Tulip Mania, (17th Century) the South Sea and Mississippi Bubbles (18th Century) and to the Florida Real Estate Bubble (20th Century) and more recently extensive mortgage and other Frauds which precipitated the US Housing Bubble which was a major contributor to the recent Financial Crisis. For more details see Insider Dealing below.

Whilst many different individuals were involved in these Frauds, some of the most notable Frauds can be attributed to individuals, particularly those creating and exploiting Ponzi Schemes; (for example the eponymous Charles Ponzi, Ivar Krueger, (20th Century) and only recently, Bernie Madoff and Alan Stanford), to those controlling major Corporate businesses; (for example Ken Lay and Jeffrey Skilling at Enron, Bernie Ebbers at Worldcom, Dennis Kozlowski at Tyco and Calisto Tanzi at Parmalat) where massive Accounting Frauds were perpetrated and to those so called Rogue Traders; (for example Nick Leeson at Barings followed by a host of others, James Jett, at Kidder Peabody, Jerome Kerviel at Soc Gen and more recently Kweku Adoboli at UBS), who placed very large unauthorised trades, which in the end led to major losses at each of the institutions involved and in the case of Barings to the collapse of what was then Britain's oldest Bank.

Money Laundering

The following, whilst certainly not exhaustive, are perhaps the most significant examples of Fraud, both in the sense of their prevalence and persistence and in terms of the size of ultimate losses to investors and to victims, categorised as to the type and nature of the Fraud involved.

Accounting Fraud Schemes

Accounting Fraud typically involves complex methods for misusing or misdirecting funds, overstating revenues, understating expenses, overstating the value of corporate assets or under-reporting the existence of liabilities, sometimes with the cooperation of officials in other corporations or affiliates.

In public companies, this type of "creative accounting" amounts to at least falsifying books and records and often to outright fraud. Such fraudulent conduct may be motivated to avoid a company's stock price from falling so as to generate profits for the high level executives orchestrating the fraud that maintain large amounts of company stock or could be done to avoid reporting instances of self-dealing by high level executives.

Accounting Fraud - Top 10 by losses			
1	<u>Enron</u>	US\$40-45bio	US
2	<u>BCCI</u>	US\$13bio	Luxembourg
3	<u>Worldcom</u>	US\$11bio	US
4	<u>Parmalat</u>	US\$10.5bio	Italy
5	<u>Olympus</u>	US\$4.9bio	Japan
6	<u>Qwest Comms</u>	US\$3.8bio	US
7	<u>Health South</u>	US\$2.7bio	US
8	<u>Bawag</u>	US\$2.6bio	Austria
9	<u>Waste Mgt</u>	US\$1.9bio	US
10	<u>Satyam</u>	US\$1.5bio	India

Source: Author

notably by those usually on the trading floor within Investment Banks, who have come to become known as **Rogue Traders**. One notable exception that is more like an Accounting Fraud than a pure Rogue Trader incident is the case of Helmut Eisner, then CEO of Austrian Bank, Bawag that made huge losses through fraudulent actions and was nearly forced into Bankruptcy.

Rogue / Unauthorised Trading

Rogue Trading is where employees - usually within Investment Banks - who are authorized to trade on behalf of their employer, but who exceed their authority. Rogue trading generally involves the entry and cancellation of fictitious orders designed to cover trading losses from unauthorised trading. As such, the practice involves multiple violations of securities and/or fraud laws as well as securities regulations. In the US, FINRA has issued guidance (See FINRA Reg. Notice 08-18) on best practices for detecting and preventing rogue trading.

These best practices include: heightened firm scrutiny of red flags such as trading limit breaches, unrealised profit and loss on unsettled transactions, unusual patterns of cancellations and corrections, a pattern of aged fails to deliver; increasing password security and other protections of firm systems and risk management information; and creating a stronger compliance culture within the firm. In the most notorious of cases they end up losing huge sums in the process for their Banks, and in the case of Nick Leeson led to the collapse of one of Britain's oldest banks, Barings Bank.

Rogue Trading - Top 10 by losses			
1	<u>Jerome Kerviel</u> Société Générale	US\$ 7.2bio	France
2	<u>Yasuo Hamanaka</u> Sumitomo Corp	US\$2.62bio	Japan
3	<u>Kweku Adoboli</u> UBS	US\$2.3bio	UK
5	<u>Frances Yung</u> CITIC Pacific	US\$1.9bio	China
5	<u>Nick Leeson</u> Barings Bank	US\$1.4bio	Singapore
6	<u>Toshihide Iguchi</u> Daiwa Bank	US\$1.1bio	US
7	<u>David Lee</u> Bank of Montreal	US\$868mio	Canada
8	<u>John Rusnak</u> Allied Irish Bank	US\$693mio	US
9	<u>Peter Young</u> DMG	US\$660mio	UK
10	<u>Joseph Jett</u> Kidder Peabody	US\$339mio	US

Source: Author

Whilst each of the rogue trading incidents have their own facts and particular circumstances, they nevertheless appear to have many similarities. For example, all are men, holding senior positions (usually MD or similar) albeit relatively young (average mid 30s when the fraud started). The duration of the fraud is approximately 3 years, with knowledge of back office operations, no evidence of active collusion but some knowledge of irregularities and a distinct absence of effective or close supervision, failing to identify and/or understand significant increases in trading activity, alleged profitability and/or trading exceptions. Motivation is largely towards establishing a stellar reputation and in so doing increasing personal compensation or starting by trying to cover for losses incurred.

The importance of these cases is to do with the huge losses incurred rather than the nature and/or provenance of the fraud. The losses that are generated by the Top 10 cases exceed US\$20bio and losses of this magnitude can hardly be contemplated by traditional forms of fraud or criminality for that matter. The link of course is that it is only as a result of the size of the Securities Markets and the nature of trading that such sums are involved and such losses can result. Beyond the odd Rogue Trader within an Investment Bank where the victim is usually his employer, there lurk plenty of other rogues looking to abuse investors in the securities and other markets, like the commodities markets, engaging in numerous forms of Market Abuse, the main areas of concern being Insider Dealing, Misuse of Information and Market Manipulation. For details see Insider Dealing which includes Misuse of Information below and Market Manipulation which is also set out in this Part 1, Section 1 below.

Hedge Fund / Investment Company Fraud

A Hedge Fund is in essence a managed portfolio of aggressive investments that uses advanced investment strategies such as leveraged, long, short and derivative positions in both domestic and international markets with the goal of reducing volatility and risk while attempting to preserve capital and deliver absolute returns to its investors under all market conditions. They are similar to mutual funds in that investments are pooled and professionally managed, but differ in that the fund has far more flexibility in its investment strategies. Alfred Winslow Jones launched the first Hedge Fund back in 1949. Mr Jones tried to minimize risk in holding long-term stock positions by short selling other stocks and he also engaged in leveraging. As the first money manager to combine short selling, the use of leverage, shared risk through a partnership with other investors and a compensation system based on investment performance, Jones earned his place in investing history as the father of the hedge fund. Since Mr. Jones' founding of the first Hedge Fund, the industry has had its ups and downs but is now running full steam with some estimates claiming over US\$2.3 trillion is managed by Hedge Funds. In most jurisdictions, Hedge Funds are often set up as private investment partnerships that are

open to a limited number of investors and require a very large initial minimum investment. Investments in hedge funds are illiquid as they often require investors keep their money in the fund for at least one year and only allow withdrawals on a quarterly, biannual or annual basis. Hedge Funds are private collective investment vehicles which are active in the global capital markets, seek to achieve absolute returns and capital appreciation. Hedge funds use a variety of investment techniques, are lightly regulated and often accept only a very limited number of investors so as to ensure that their investment strategy remains flexible. Hedge funds are categorized not only according to the asset classes in which they invest (equities, bonds etc.) or their geographic or thematic orientation, but also in terms of their strategies (e.g. arbitrage, macro, event-driven or opportunistic). Hedge Funds are Pooled Investment Vehicles.

The theory behind their creation was that wealthy investors are "financially sophisticated" and therefore do not need as much regulatory protection. It is this absence of regulatory scrutiny that poses risks in dealing with Hedge Funds and which may tempt unscrupulous hedge fund managers to commit fraud and/or tempt the introduction of criminal proceedings. Whilst there have not been many cases of hedge funds being used as vehicles for money laundering or terrorist financing, there have been many instances of hedge fund managers, especially in the past three to five years, accumulating insider information and using it to increase returns on investments and gain an edge in the highly competitive hedge fund industry. In addition, because of the opaque nature and structure of a hedge fund, they have a propensity to be embroiled in Ponzi schemes. Fund managers can easily create an illusion of positive returns and they can easily falsify statements with exaggerated assets under management to investors. In 2011 one of the 'largest hedge fund insider trading cases in US history' came to an end when Galleon hedge fund manager Raj Rajaratnam was convicted of insider trading. He created an intricate system of insiders across the financial industry that he used to access information to benefit his hedge fund. For more information about Insider Dealing and/or Market Manipulation see below. At Daedalus Capital Partners, for example, a classic Advanced Fee scheme was perpetrated by the hedge fund manager; investors received false financial statements claiming large profits, when in fact the money was being siphoned off and used to finance the manager's lavish lifestyle. Another example was the Hedge Fund Group known as the Bayou Funds which was run by Samuel Israel III which also collapsed following Israel's attempts to make money to cover a loss by overtrading, losing still more money and failing to disclose the real state of the Fund until its collapse. Israel nearly further compounded his Investors losses by trying to be the remaining funds on offered Prime Bank Instruments, itself a scam tried out on Israel himself but the trades didn't go through when the custodian Banks refused to move the money and informed the authorities.

Boiler Rooms

Boiler Rooms refer to a busy centre of activity, usually selling speculative, questionable, worthless or non-existent securities traditionally by telephone, where a group of salesmen work using unfair, dishonest high pressure sales tactics or committing outright fraud. The term "Boiler Room" is likely to have originated from the cheap, hastily arranged office space used by such firms, often just a few desks in the basement or utility room of an existing office building or by the high pressure heating appliances or a combination of the two. Whilst many consider boiler rooms a fictional relic of a bygone era, for example many disappeared in the 1990s following the burst of the "dot-com bubble," many boiler rooms still operate across the world. Advances in telecommunication technology mean that a company can viably operate from long distances targeting unsuspecting prospective investors. Also the Internet has led to this medium being abused for securities frauds by mimicking traditional telephone scams, and leveraging the Internet to provide increased anonymity and increased targeting of investors.

Boiler Rooms may also operate in one country while calling prospective investors in another. The advantage of such an operation is that a company can often operate without fear of prosecution from the investor's native legal system. For example, many boiler rooms contacting prospective investors in the UK operate from Spanish cities such as Barcelona and Valencia.

A recent example would be the case of David Mason who was arrested and sentenced to 2.5 years in prison in the UK. Mason organised cold calling to sell shares in a company EduVest which he had set up himself and was worthless, taking £270,000 from 32 investors. Another example of Boiler Room activity was Stratton Oakmont a New York brokerage house founded by Jordan Belfort and Danny Porush that was shut down in the late 1990s, following numerous complaints. The brokerage perpetrated one of the oldest scams in stock market history, the Pump and Dump, buying up large amounts of shares in a thinly-traded company, recruiting hundreds of others to do the same (often not revealing the large ownership stake) in order to raise the stock's market value, and then selling the shares at the inflated price before the other shareholders are aware of the scheme. Belfort was convicted of securities fraud in 1999 and served 22 months of a four-year sentence.

Prime Bank Instruments/Schemes

Investors are induced to invest in financial instruments, allegedly issued by well-known institutions, which offer risk-free opportunities for high rates of return; benefits which are allegedly the result of the perpetrator's access to a secret worldwide exchange ordinarily open only to the world's largest financial institutions. Prime Bank Instruments or Guarantees are bogus instruments and a form of High Yield Investment Fraud, which themselves take many forms, but are all characterized by offers of

low or no risk investments that guarantee unusually high rates of return. They also include Ponzi Schemes.

Investment Frauds

Investment / Ponzi Schemes

Named after its early 20th century creator, Charles Ponzi, these schemes use money collected from new 'investors' (i.e., victims), rather than profits from the purported underlying business venture, to pay the high rates of return promised to earlier victims. This arrangement gives victims the impression that there is a legitimate, money-making enterprise behind the perpetrator's story when, in reality, victim monies are the only source of funding. Classic major investment fraud schemes often rely on attracting investors based on false promises/representations of high rates of returns on investments. The more significant cases often involve people that, until the unraveling of the fraud, are projected as successful prominent businessmen. For example, Bernie Madoff, who orchestrated the largest ever Ponzi scheme, ran his own US registered broker dealer and Investment Advisory firms, and had served as Chairman to the Board of Directors and on the Board of Governors to NASDAQ, a Self Regulatory securities industry organisation. Similarly, Alan Stanford, ran his own banks and had been knighted by Antigua and Barbuda. The fraudsters who orchestrate an Investment Scheme often illegally use investor funds for their own personal benefit to purchase luxury items and project a high style of living. This in turn is often used to attract other investors. In reality their "success" is illusory, the investments are either never made or simply never perform to the represented returns. The fraud is usually perpetrated by providing false statements to customers. Outside of Bernie Madoff, which involved a classic Ponzi scheme that was furthered by providing his clients false returns on investments purportedly made in the stock market, more often the investments are less transparent, such as promissory notes, or other securities created by the fraudster. In such schemes, the activity flowing through a financial institution will show an inflow of funds from the investors and an outflow to different investors. The fraudster may use multiple accounts and different institutions to further conceal the fraud. For more details and case examples see, Charles Ponzi, Ivar Krueger, Bernie Madoff and Alan Sanford.

Some Investment or Ponzi schemes revolve around a specific product, that while legal, is susceptible to fraud if unregistered or less transparent, such as Promissory Notes; overly complex, such as Securitized Life Settlement Contracts; marketed as being mysterious or for special investors, such as Gold and Precious Metals or energy Investments; or preys on the desperate, such as Distress Real Estate schemes. Other schemes, referred to as Affinity Fraud, may target a particular group of people who are similar to, or have something in common with, the fraudster, as was the case with Bernie Madoff.

Ponzi Schemes - Top 10 by losses			
1	Bernie Madoff	US\$10-17bio	US
2	MMM Company	US\$10bio	Russia
3	R Allen Stanford	US\$8bio	US / Antigua
4	Tom Petters	US\$3.75bio	US
5	Scott W Rothstein	US\$1.4bio	US
6	Albania Lottery Scheme	US\$1.2bio	Albania
7	Damara Bertges & Hans Gunther Spachtholz	US\$1.1bio	Germany & Switzerland
8	Caritas (Charity)	US\$667mio	Romania
9	Reed Slatkins	US\$593mio	US
10	Gerald Payne	US\$500mio	US

Source: Author

The Pyramid Scheme

As in Ponzi Schemes, the money collected from newer victims of the fraud is paid to earlier victims to provide a veneer of legitimacy. In Pyramid Schemes, however, the victims themselves are induced to recruit further victims through the payment of recruitment commissions.

Nigerian Letter (419) /Advance Fee/Lottery Frauds

This category of fraud encompasses a broad variety of schemes which are designed to induce their victims into remitting up-front payments in exchange for the promise of goods, services, and/or prizes. These fraudulent schemes are typically not sophisticated and the victim is induced to send funds in return for a promise of larger return.

Advance Fee Fraud

In a typical Advance Fee Fraud the fraudster solicits their victim through unsolicited means (Internet, mail) indicating that they have funds due to them (lottery, inheritance) and must send their own funds in order to claim/release these winnings. Prosecutions of such crimes are infrequent given the logistical challenges of tracing the fraudsters who often operate outside of the jurisdiction of the victim. The impact of such schemes are nonetheless devastating to the victims who can lose significant assets and in some instances their life savings. The crimes are likely under-reported given the victim's humiliation at falling prey to such schemes. Because these schemes pose a low risk of prosecution while also generating significant proceeds, they are utilised by certain criminal organisations in Africa, and in particular Nigeria where they are known as '419 letters' after the section of the Nigerian Penal Code referring to such crimes. A fraudster who employed Advance Fee Fraud

techniques and who currently sits in an Indian jail and is the subject of a major probe is [Hassan Ali Khan](#). Perhaps the most successful case using some of these techniques is the case of [Chief Nwude](#) who was able to steal US\$242mio from Brazilian Bank Noroeste. For more details see also Part 2, Section 5, Nigerian Crime Gangs.

Some of the most prevalent Advance Fee Fraud schemes being encountered include the following:

Disaster Fraud

When a disaster occurs, there are many organisations and individuals soliciting contributions for the victims of this disaster. Most of the organisations and individuals involved are legitimate; however, there are some who are not. Victims may be approached by unsolicited e-mails asking for donations to a legitimate-sounding organisation. The schemer will instruct the victim to send a donation via a money transfer. Other types of disaster fraud include false or exaggerated claims by policyholders; misclassification of flood damage as wind, fire, or theft; claims filed by individuals residing hundreds of miles outside the disaster zone; bid-rigging by contractors; falsely inflating the cost of repairs; and contractors requiring up-front payment for services, then failing to perform the agreed upon repairs

Foreign Lottery Fraud

Victims are informed they have won a substantial prize in a foreign lottery usually by e-mail, but before they can collect or receive the winnings they must first make some payments for example to cover taxes or other fees. Alternatively, victims are provided with counterfeit financial instruments, which can be cashed only by first paying a fee.

Overpayment Fraud

Victims who have advertised an item for sale are contacted by bogus buyers who remit counterfeit financial instruments, in excess of the purchase price, for payment. The victims are told to cash the instruments, often a cheque, but first send the difference between the price of the goods and the overpayment to the buyer, often by wire so that the victim's payment clears before the fraudulent instrument is determined to be bogus..

Recovery Schemes

Victims that have already succumbed and lost money are seen as particularly vulnerable and attempts are often made to reconnect with the victim to try to defraud him even further, often by trying the Recovery Scheme. The Victim is contacted by people posing as police officers, government employees, or lawyers informing victims that the persons responsible for the original fraud schemes have been arrested or successfully sued and their bank accounts have been seized. The victim is told the seized money is going to be returned to him, but the victim must first pay fees for processing and administrative services. Recovery schemes often target victims many months or years after the original fraud schemes.

Banking/Payment Card Fraud

This is a generic term used to describe a range of offences involving theft and the fraudulent use of accounts payment and card account data. Frequent types of banking fraud and payment card fraud include:

PB Fraud/Broker Embezzlement

As with Rogue Traders in Investment Banks, Client Advisers in Private Banking operations have been known to act outside of their authority, for example by acting either on a discretionary basis or on a purely fraudulent basis, by trying to cover unauthorized losses or by trying to defraud a client or clients of their own assets. An example of one that began as the former and turned into the latter is the case of [Hans Peter Walder](#), a private banker with access to client funds.

There are other similar frauds that arise out of relationships where there should exist a high level of trust, for example by trustees or lawyers and/or bookkeepers. Kenneth Starr is a good example. He was a former CPA and attorney convicted of running a US\$30mio Fraud scheme with the money of numerous wealthy and celebrity clients. In May 2010, Starr was indicted and arrested on 23 criminal counts, including various fraud and money laundering charges. In September 2010, Starr pleaded guilty in federal court and was sentenced in March 2011 to a 7.5-year prison term that he is currently serving and is due to be released in 2016. Starr initially made large amounts of money for clients, but he eventually began using client assets to fund his personal expenses, as well as high-risk investments in which he and his associates had financial interests. As his personal expenses increased and various high-risk investments failed, Starr began stealing funds from older clients and using subsequent investment from new clients to cover up the prior thefts. One of those clients was 93-year-old former actress Joan Stanton, after obtaining a power of attorney over her assets, Starr then depleted her funds and was subsequently sued by her in civil court in April 2008. After Stanton died in 2009, Stanton's daughter launched a federal criminal investigation of Starr, which led to the uncovering of his multi-million dollar Fraud. In these cases the fraudster has access to the funds through their fiduciary relationship with the victim.

Credit & Debit Card Fraud (incl Counterfeit Cards)

Credit card fraud is the illegal obtaining of goods or services, or to obtain unauthorised funds from an account by using another persons credit card or any similar payment mechanism (for example, debit cards, store cards, etc.) as a fraudulent source of funds in transaction. This can be done by creating a copy of a card, 'skimming' the details during a routine transaction, stealing a card or intercepting it in the post and many other creative ruses. Credit card fraud is often committed in addition to identity theft. Counterfeit card fraud is undertaken using plastic cards that have been specifically produced or existing cards that have been altered. These cards are encoded with illegally obtained payment

card account data in order to pay for goods and services or to withdraw cash. Card not present (CNP) fraud is committed using payment card account data to undertake transactions where there is no face-to-face contact between the seller and purchaser. Typically, this type of fraud is committed over the Internet, by mail order or telephone. CNP fraud is currently one of the fastest growing payment card related types of fraud.

Cheque Kiting

Cheque Kiting is a cheque fraud scheme taking advantage of the float time (the bank's delay in the clearing process between receipt of deposits and cheques and their processing) to defraud banks by writing cheques against accounts with insufficient funds to cover the cheque. This is been done by writing a cheque to the criminal from one bank and depositing and even crediting it to an account at another bank. The account with the credited cheque shows then a positive balance, which enables the criminal to withdraw enough money to deposit back into the first bank before the cheque bounces for lack of funds. Banks should use an electronic receipt system to reduce the float time by instantly recording and processing cash transactions

Identity Theft / Bank Account Takeover

Identify theft is the stealing of a person's financial or personal information, especially credit cards and Social Security numbers or other identification numbers or data often through Phishing or Pharming techniques, with the intention of using that data to commit fraud and create a duplicate persona. There are some methods that involve accessing a person's computer and obtaining passwords and access information or using some of the weaknesses in the Internet often in an effort to "take-over" a bank account or access other financial accounts. Others involve attacking corporate computer and database systems to get access to the information that they hold on customers, such as bank account information or even social applications like Twitter that sometimes copy and store customer information without their knowledge (e.g. smart phone contacts.)

Mortgage and Other Credit / Loan Frauds

Mortgage Fraud and/or Loan Fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction in the case of a mortgage or a credit transaction in the case of a loan. The most common misrepresentation relates to overstating income and asset information on a loan application. Whilst the perpetrator of the Fraud is usually the borrower, there are cases where one or more industry insiders or professional parties assist using their specialized knowledge or authority to commit or facilitate the fraud. For example, in the case of real estate mortgage fraud, particularly systemic frauds, it is not surprising to find collusion by bank officers, appraisers, mortgage brokers, lawyers, loan originators, and other professionals engaged in the industry. Fraud for housing typically represents illegal actions conducted solely by

the borrower, who is motivated to acquire and maintain ownership of a house under false pretenses such as misrepresented income and asset information on a loan application.

Trade Based Money Laundering

One of the 3 primary methods used by criminals to move criminal money involves trading goods, alongside moving cash and other valuables outside the formal financial sector and cash and other valuables inside the formal financial sector. These methods can also be used in various combinations.

The method involving goods is known as “trade-based money laundering.” It involves the transfer of “value” via commodities and trade goods, either to avoid customs and excise or other duties or taxes or otherwise minimizing taxable income or to provide a “counter-valuation” or a way of balancing the books in many global underground financial systems. It is also a mechanism to enable capital flight or foreign inward investment.

The Financial Action Task Force (FATF) defines trade-based money laundering (TBML) as the “process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.” Trade-based money laundering techniques take a wide variety of forms.

For example, at its most basic it could be a simple bartering or a commodity for commodity exchange. In certain parts of Afghanistan and Pakistan the going rate for a kilo of heroin is a color television set. Drug warlords exchange one commodity they control (opium) for others that they desire (luxury and sports utility vehicles). More sophisticated however is the manipulation of goods traded, particularly goods destined for overseas buyers.

It is important to understand that when a buyer and seller are working together, the price of any good can be whatever they want it to be and so simple invoice fraud is an easy and effective way of money laundering.

Under Invoicing/Over Invoicing

Simple invoice fraud and manipulation involves the misrepresentation of the trade good in order to transfer value between an importer and an exporter. The quantity, quality, and description of the trade goods can be manipulated. The shipment of the actual goods and the accompanying documentation provide cover for “payment” or the transfer of money. So for example to move money out: Import goods at overvalued prices or export goods at undervalued prices; and to move money in: Import goods at undervalued prices or export goods at overvalued prices. As long as parties in an international trade transaction do not get too aggressive or greedy and cause noticeable trade anomalies, their chances of detection by customs services, law enforcement and other authorities appear low.

According to the US State Department, this practice has reached “staggering” proportions in recent years. The US Department of Treasury estimates that the [Black Market Peso Exchange](#), a Trade Based Money Laundering methodology found in the Western hemisphere, launders billions of drug dollars every year. For more details see Part 1: Section 1 Drug Trafficking.

Other Countries particularly effected include Brazil, Russia, India and China. According to Global Financial Integrity (GFI), a Washington, DC-based research and advocacy organisation, in its study, entitled “Russia: Illicit Financial Flows and the Role of the Underground Economy,” it estimated that the Russian economy lost US\$211.5bio in illicit financial outflows from 1994 through to 2011, whilst at the same time received illicit inflows to the Russian economy of US\$552.9bio over the same time period.

A similar study published by the Institute on China estimated that US\$3.79 trillion in illicit financial outflows occurred from the Chinese economy from 2000 through 2011. (“Illicit Financial Flows from China and the Role of Trade Misinvoicing.”) GFI Director Raymond Baker stated that “There’s no other developing or emerging economy that even comes close to suffering as much in illicit financial outflows.”

The research found that the illegal outflows, the proceeds of crime, corruption, and tax evasion were largely due to a trade-based money laundering technique known as ‘trade misinvoicing,’ which accounted for US\$3.2 trillion, or 86.2%, of the total outflow of illegal capital over the 11 years studied. The research found that there had been a sharp increase in annual illicit financial outflows, increasing from US\$172.6bio in 2000 to US\$602.9bio in 2011.⁸

Countering Trade Based Money Laundering

Whilst detection rates considered historically low, increased attention to countermeasures have been considered and there is cause to believe that detection rates should improve in the near future. Every country has a customs service and tracks what comes in and what goes out.

In fact, in many parts of the world, customs duties are the primary source of government revenue. So although there are differences in the way governments gather and store trade data, enough similarities exist to conduct effective analysis and TBML investigations. Such investigations require three basic elements: (i) Access to import and export data; (ii) the ability to exchange data with other countries; and (iii) expertise in analyzing and investigating TBML.

Recognising the growing threat of TBML, in 2004 the Department of Homeland Security’s Immigration and Customs Enforcement (ICE) established the world’s first trade-transparency unit or TTU. Subsequently,

other TTUs have been created in Argentina, Brazil, Paraguay, Colombia, Panama, Mexico and other countries. By comparing one country’s imports or exports against the corresponding data of another country, trade anomalies can be detected that could be indicative of customs fraud, tax evasion and capital flight contraband smuggling or trade-based money laundering. This data could even be the back door into underground financial systems.

For example, a TTU looked at import and export data between two countries, and may identified that fluctuating values were associated with the values ascribed to refrigerators exported from one country to another. Whilst refrigerators were exported from Country A largely at one value, their value declared on import in Country B was much greater. In this case, the value transfer represented by the shipments of refrigerators masked the laundering of the proceeds of narcotics.

Tax Evasion/Tax Fraud

Tax evasion is the general term for efforts by individuals, corporations, trusts and other entities to evade taxes by illegal means. Tax evasion usually entails taxpayers deliberately misrepresenting or concealing the true state of their affairs to the tax authorities to reduce their tax liability and includes in particular dishonest tax reporting, such as declaring less income, profits or gains than actually earned or overstating deductions.

Tax evasion is an activity commonly associated with the informal economy and one measure of the extent of tax evasion is the amount of unreported income, namely the difference between the amount of income that should legally be reported to the tax authorities and the actual amount reported, which is also sometimes referred to as the tax gap.

In the US, the IRS estimate of the 2000 tax gap was US\$385bio.⁹ A more recent private study estimated the tax gap as US\$500bio.¹⁰ Therefore, 18-19% of total reportable income is not properly reported to the IRS, it is estimated that global tax evasion could amount to 5% of the global economy. Aside from figures, that relate to tax evasion or abusive tax avoidance where for example, the European Commission has reported in 2012 that tax evasion activities within the 27 nation EU amounted to a loss of US\$1.3 trillion.¹¹

Tax fraud is an even more serious crime, usually involving organised criminal gangs, targeting tax laws to generate significant criminal proceeds. The largest tax fraud market is that which focussed on EU VAT Fraud. Those who perpetrate VAT fraud, are becoming increasingly sophisticated in their methodologies.

Currently, organised criminal groups, based both within and outside the EU, are orchestrating large scale attacks on EU Member States’ exchequers by carefully monitoring “the market” for further opportunities offered by diverse commodities or deregulation of certain mar-

kets, such as the gas and electricity sectors. Organised criminal groups almost routinely employ the knowledge of specialised facilitators and mechanisms, frequently situated outside the EU, to mask their fraudulent activities, take advantage of loopholes in legislation governing financial practices and ultimately trawl the plethora of schemes and safe havens available to launder the proceeds of their crimes. VAT fraud alone in the EU costs Member States approximately €100bio a year, according to Europol.

MTIC/Carousel Fraud

Cross-border transactions within the EU have, since 1992, been zero-rated for VAT. Importers of goods are thus able to receive goods without paying VAT, but charge VAT on their resale. If the VAT they receive is not then remitted to the revenue authority, they are committing a crime. This crime is known as “Missing Trader Inter Community Fraud.”

The schemes are based on either virtual or real ‘carousel’ transactions where the same ‘goods’ are sold and resold several times. This is commonly referred to as VAT “Carousel Fraud.”

Attempts to undertake this fraud have risen considerably in the past decade, largely due to the proliferation of high value and low weight goods, or service industries, usually with few barriers to entry such as mobile phones and computer chip, although the subject of the fraud has diversified for example with cosmetics, “precious” metals and computer Software being targeted by criminals.

The basic model of transnational intra-community VAT fraud involves at least two Member States. MTIC is carried out by organised criminals who put in place a structure of linked companies and individuals whilst at the same time exploiting the different particularities of national tax systems to disguise the real links between participants. Those involved in VAT fraud schemes, who are initially responsible for the tax damage, the so-called missing traders only operate for a short time, sometimes only weeks, before disappearing.

Whilst this is a fraud against the fiscal authorities of the EU Member States, cross-border, or transnational, VAT fraud not only affects the economic and financial interests of the EU but also has an impact on lawful businesses which in turn may have a negative impact on employment levels. Moreover, the profits from VAT fraud may finance other types of criminal activity, for example cigarette smuggling or drug trafficking.

Major VAT fraud has been detected in the trading of emission allowances or European unit allowances (EUAs). Europol estimates that the loss to carbon credit fraud between June 2008 and December 2009 was approximately €5bio.¹²

Cybercrime

In a world awash with information, cyberspace is a new frontline in the war on crime. Already one third of the world's population has access to the internet, and with this comes growing cybercrime. A recent study from Ponemon Institute has found that the average cost related to cybercrime for 50 US companies was US\$5.9mio per year. This represents an increase of 56% from the first cyber cost study published in 2010. It took an average of 14 days and US\$247,744 to clean up an attack in 2010. In 2011, with a jump in stealth tactics, that average increased to 18 days, and the cost climbed to US\$417,748. More than 90% of all cybercrime costs were caused by malicious code, denial of service, stolen devices and web-based attacks.¹³

Cybercrimes can be defined as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical financial or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, e-mails, notice boards and groups) and mobile phones (SMS/MMS)".

As far as computers go cybercrime encompasses a broad range of activities. Generally, however, it may be divided into two categories: (i) crimes that target computers directly; (ii) crimes facilitated by computer networks or devices, the primary target of which is independent of the network or device. Crimes that primarily target computer networks or devices include: Computer viruses; Denial-of-service attacks; Malware (malicious code) whilst crimes that use computer networks or devices to advance other ends include: cyberstalking; Fraud and identity theft; Information warfare; and Phishing scams and of course Spam, (or the unsolicited sending of bulk e-mail for commercial purposes, which is unlawful in some jurisdictions).

Cybercrime is not only targeted at companies, governments and other public institutions or simply on or via computer devices. 69% of online adults have been a victim of cybercrime in their lifetime. Of these, 10% have experienced cybercrime on their mobile phone and 42% more mobile vulnerabilities were reported in 2010 compared to 2009, a sign that cybercriminals are starting to focus their efforts on the mobile space. In addition to threats on mobile devices, increased social networking and a lack of protection are likely to be some of the main culprits behind the growing number of cybercrime victims.¹⁴ According to SANS Technology Institute¹⁵ one of the biggest 2011-2012 security issue seems to be apps with spyware. Even the apps that come loaded on your phone are potentially a problem. The security issue is that your smartphone knows where you are, has access to your e-mail, appointments, phone contacts, and is part of the way you surf the web, make purchases, access your bank account, yet has very little security or privacy built into it.

Cybercrime includes threats from both cyber spies and cyber criminals as well as activists and pranksters. The cyber threat has evolved and grown significantly over the past decade. Cyber spies, criminals and hackers have become increasingly adept at exploiting weaknesses in computer networks and mobile systems.

Cyber Terrorism

Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern that such intrusions are part of an organised effort by cyberterrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. The US Department of Defence (DoD) notes that cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. The DoD stated that, "In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by war-fighting military commanders in the future."

Organised Crime

Beyond cyber terrorism are hackers-for-profit, who do not seek information for political power, rather they seek information for sale to the highest bidder. These once-isolated hackers have joined forces to create criminal syndicates or to work directly with organised criminal gangs. Operating in cyber space appears to offer good profits with a lower probability of being identified and prosecuted.

For example, Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs.

Organised criminal gangs are also involved in cyber extortion, where a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks. According to the Federal Bureau of Investigation, cyberextortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI but many

more go unreported in order to avoid publicity.

The following are recent examples of criminal activity identified and shut down by law enforcement.

In April 2011, the Coreflood botnet was identified and finally dismantled. This botnet infected an estimated two million computers with malware that enabled hackers to seize control of the privately owned computers, to steal personal and financial information. Botnets are networks of virus-infected computers controlled remotely by an attacker. They can be used to steal funds, hijack identities, and commit other crimes. The botnet in this case involved a virus with a key-logging programme that allowed cybercriminals to steal personal and financial information by recording unsuspecting users' every keystroke

More recently a criminal network operated by an Estonian company called Rove Digital were caught manipulating Internet "click" advertising. They redirected users from legitimate advertising sites to their own advertisements and generated more than US\$14mio in illegal fees. This "click" scheme impacted more than 100 countries and infected four million computers.

One of the most audacious cybercrimes was committed in 2008 when an organised group of criminals, using cloned or stolen credit and debit cards and PIN's to go with them, hit more than 2,100 ATMs in at least 280 cities on three continents, in such countries as the U.S., Canada, Italy, Hong Kong, Japan, Estonia, Russia, and the Ukraine at the same time! When it was all over in only 12 hours, the criminals had stolen US\$9mio in cash, which would have been more, had the targeted ATMs not been drained of all their money.

The masterminds of this scheme were three 20-something Eastern Europeans and an unnamed person called simply "Hacker 3." Working together, the four hackers hatched "perhaps the most sophisticated and organised computer fraud attack ever conducted," according to Acting US Attorney Sally Quillian Yates of the Northern District of Georgia. It started when a 28-year-old Moldovan man learned of a vulnerability in the computer network of a major credit card processing company based in Atlanta. With an eye toward exploiting it, he passed that information to a hacker living in Estonia. The Estonian conducted "reconnaissance" on the network vulnerability and shared what he learned with a hacker in Russia. With the help of the three other hackers at varying times, the Russian was able to break into the electronic network, reverse-engineer the PIN codes from the encrypted system, and raised the limits on the amount of money that could be withdrawn from the prepaid payroll debit cards. (These cards, used by many companies, enable employees to withdraw their salaries from an ATM.) In addition to providing computer support, Hacker 3 managed the network of thieves around the world, called "cashers" who used a total of 44 counterfeit cards to withdraw the US\$9mio.

The Estonian also managed his own cashing group. As the cashers went to work, the Russian took the lead in monitoring the victim company's database to track the illegal withdrawals. With the Estonian, he later deleted or tried to delete files on the computer network to cover their tracks. When the ATM thefts were complete, Hacker 3 with the help of the Estonian gathered and divvied up the proceeds. The cashers got to keep 30 to 50% of the money they stole; the rest went to the four hackers.

Another example of cyber criminal activity was when a group of cyber criminals established a forum on the Internet called "Dark Market," where they bought and sold stolen financial information such as credit card data, login credentials (user names and passwords), and even electronic equipment for carrying out financial crimes. At its peak, this vast criminal network had over 2,500 registered members. Dark Market was like an exclusive club for cybercriminals a meeting place for getting cyber criminal advice and arranging deals. The Market was taken down after being infiltrated by law enforcement.

Cybercrime appears to be the fastest growing sector of organised crime activity with growth rates in excess of 25% annually. Industry as well as computing has always had its clusters, locations where expertise is found and where others co locate to contribute and leverage. In the area of cybercrime, clusters have also developed and the leading countries where such criminals reside and operate are Brazil, Russia and its former soviet republics and China, with India catching up. These countries have something in common which is attractive to the cybercriminals, which allow them a certain expertise and some freedom to more easily operate than in some other locations. These are, (i) high levels of poverty and unemployment; (ii) a high standard of basic education; and (iii) a significant presence already of organised criminal gangs.

Whilst the largest threat appears to come from Russia, according to Group IB in their report entitled, " State and Trend of the Russian Digital Crime Market"¹⁶ they found that whilst the global market was worth some US\$12.5bio, the Russian's controlled around US\$4.5bio of the total. The largest type of Russian cybercrime was online fraud valued at US\$942mio, followed by spam at US\$830mio; C2C (including services for anonymisation and sale of traffic, so called exploits, malware and loaders) at US\$230mio and denial of service attacks at US\$130mio.

According to the UK National Audit Office, most recent figures put the cost to the UK economy for example of losses from and costs to prevent cybercrime amounted to between £18-27bio.¹⁷

Human Trafficking

"I was 14 and they took me and my cousin - they poured petrol over her and burnt her and made me watch her die. I was made to look after a little boy about six and he cried for his parents but I had to tell him he would not see them again". This was the testimony of a girl made to a Mexican NGO in 2010 who was forced into prostitution

Harms

Human trafficking is a form of modern-day slavery where people profit from the control and exploitation of others. Many victims of human trafficking are forced to work in prostitution or the sex industry. But trafficking also occurs in forms of labour exploitation, such as domestic servitude, restaurant work, janitorial work, sweatshop factory work and migrant agricultural work. Apart from the long-term physical & psychological damage that may occur to the individuals and families involved in human trafficking, there are other harms that are less obvious. Consumers that utilise these services are supporting the traffickers and allowing their criminal enterprises to continue to expand. Trafficking of humans is the third largest criminal industry in the world, and, according to some, the fastest growing.

Statistics

According to the UNODC 2006 report on global patterns of human trafficking, governments reported human trafficking originating from 127 countries and exploited in 137 countries worldwide from 1996 to 2003.¹ According to the UN Trafficking in Persons Report 2010² around 12.3 million adults and children are forced into slavery via forced labour, bonded labour and prostitution around the world. It is estimated on this basis that today there are more slaves on the planet than at any other time in History. The ILO has assessed that at least 12.3 million people worldwide are victims of forced labour, with the UN assessing that around 2.5 million of these are as a result of human trafficking. Other estimates from the US Agency for International Development (USAID) for example put the figures even higher, with it estimated that up to four million women, children and men are trafficked each year.

The UN Office on Drugs and Crime considers people trafficking as the fastest growing means by which people are enslaved, the fastest growing international crime, and one of the largest sources of income for organised crime. Trafficking is a multi-billion dollar business, and by its very disguised and hidden nature the precise statistics on trafficking are very difficult to estimate. The Council of Europe have made clear that;

"People trafficking has reached epidemic proportions over the past decade, with a global annual market of about US\$42.5bio." The International Organisation for Migration (IMO) has put the majority of trafficking victims as between 18 and 24 years of age, with UNICEF estimating that around 1.2 million children are being trafficked each year for purposes of sexual exploitation. Of those victims used for forced sexual exploitation it is estimated by the International Labour Organisation (ILO) that 98% are women and girls. Women and girls trafficked for labour exploitation also frequently encounter and endure sexual violence, with estimates that 95% of victims experience physical or sexual violence during trafficking.

Common abuses experienced by trafficked persons include rape, torture, debt bondage, unlawful confinement, and threats against their family or other persons close to them as well as other forms of physical, sexual and psychological violence. The International Labour organisation (ILO) estimates that criminal networks generate revenues of US\$32bio per year with the "human being as a commodity". According to the ILO, half of this profit is made in industrialised countries (US\$15.5bio) and close to one-third in Asia (US\$9.7bio).³

Proceeds of Human Trafficking		
1	Prostitution	US\$187bio
2	Human Trafficking	US\$32bio
3	Human Smuggling	US\$20bio
4	International Adoptions	US\$1.3bio
5	Organ Trafficking	US\$75mio
Estimated Total		US\$240bio

Source: Havocscope⁴

Definition / Description

Human trafficking is the illegal trade of human beings for the purposes of commercial sexual exploitation, including prostitution and child sexual exploitation, forced labour and organ removal. Human Trafficking is one of the fastest growing and most insidious and harmful criminal industries in the world, controlled largely by organised crime and amounting to a modern-day form of slavery. Traffickers use various techniques to instill fear in victims and to keep them enslaved. Some traffickers keep their victims under lock and key. However, the more frequent practice is to use less obvious techniques including: debt bondage - financial obligations, honor-bound to satisfy debt; isolation from the public - limiting contact with outsiders and making sure that any contact is monitored or superficial in

nature; isolation from family members and members of their ethnic and religious community; confiscation of passports, visas and/or identification documents; use or threat of violence toward victims and/or families of victims; the threat of shaming victims by exposing circumstances to family; telling victims they will be imprisoned or deported for immigration violations if they contact authorities; control of the victim's money, e.g., holding their money for "safe-keeping".

Historical Background / Context

From the ancient Greek and Romans to the medieval times, and up until today, humans have been subject to various forms of physical and sexual slavery.

Although forms of slavery existed before the 1400, the 1400s marked the start of European slave trading in Africa with the Portuguese transporting people from Africa to Portugal and using them as slaves. In 1562, the British joined in on the slave trade in Africa. The development of plantation colonies increased the volume of the slave trade. Later on throughout the 1600s, other countries became more involved in the European slave trade. These included Spain, North America, Holland, France, Sweden, and Denmark and would remain legal until the 19th Century.

In 1904, the International Agreement for the Suppression of "White Slave Traffic" was signed and put into action. The purpose of this agreement was to protect women, young and old, from being involved in so called "white slave traffic." White slavery referred to forcing a white woman or girl into prostitution. The agreement stands as a moral action against the trafficking of women.

In 1927 and onwards, The League of Nations, founded after WWI, amended the Suppression of White Slave Traffic to "traffic in women and children" so that everyone was included with no discrimination to race. Children of both genders were also recognised as victims of trafficking. In addition, two major studies were conducted, one in the West and one in the East, in an attempt to find out the real status of trafficking in these areas. Factors that were measured included the number of women engaged in prostitution, the demand, and the surrounding environment of the women who were trafficked.

During WWII, Japan had set up a horrifying and outrageous system where women all across Asia were forced into sexual slavery. The women were housed in what were known as "comfort stations." The conditions in these stations were atrocious, with each woman detained in a small cubicle, and received beatings and

other tortures if they were defiant. Because of this, many women ultimately died of disease, malnutrition, exhaustion, suicide, etc. The stations were also surrounded by barbed wire, making escape impossible. The Japanese government set up these stations in hopes of preventing rape crimes in public, prevent the spread of STDs, and to provide comfort for soldiers so they wouldn't tell military secrets.

In 1956, India initiated the Immoral Traffic (Prevention) Act, which persecutes those involved in trafficking. These activities included running brothels, living on earnings from sex work, capturing and imprisoning people into prostitution, etc, building on examples of such laws being enacted around the world. In 1995, the UN held the fourth World Conference to address the issue of trafficking of women. In this meeting, trafficking was actually recognised as an act of violence against women, and the concept of trafficking was further defined. Most importantly, actions to be taken included enforcing conventions on trafficking and human slavery, addressing the factors that encourage trafficking, setting up effective law enforcement and institutions who would work to eliminate trafficking both nationally and internationally, and implementing programmes including educational and rehabilitation institutions to provide for the social, medical, and psychological needs to victims of trafficking.

Notwithstanding increased focus, trafficking appears to be increasing, with many examples, beyond trafficking for sex to also include economic migrants smuggling. In 2008, for example, 57 migrants were illegally smuggled into Thailand. Fifty-seven of these migrants suffocated to death while being transported after being confined in a sea container where the air-conditioning system malfunctioned. There were 67 survivors. The driver ignored protests by the passengers, fearing that the police would be suspicious at checkpoints, and fled the scene when concerns were raised.

Money Laundering

A distinction can be made between people smuggling as a service to those wanting to illegally migrate, and the involuntary trafficking of people. An estimated 90% of people who illegally cross the border between Mexico and the US are believed to have paid a smuggler to lead them across.⁵ Trafficking in human beings, for sexual services, sex trafficking, is not the same as people smuggling. A smuggler will facilitate illegal entry into a country for a fee, but on arrival at their destination, the smuggled person is free; the trafficking victim is coerced in some way. Victims are tricked or lured into being trafficked by false promises, or forced into it. Traffickers use coercive tactics including deception, fraud, intimidation, isolation, physical threats and use of force, debt

bondage or even force-feeding drugs to control their victims. While the majority of victims are women, and sometimes children, other victims include men, women and children forced or conned into manual or cheap labour. Due to the illegal nature of trafficking, the exact extent is unknown.

Smuggling is also reaping huge financial dividends to criminal groups who charge migrants massive fees for their services. Drug-traffickers and other criminal organisations are switching to human cargo to obtain greater profit with less risk. The smuggling of people is a growing global phenomenon and it is not only a transnational crime, but also an enormous violation of human rights and a contemporary form of slavery. Currently, economic instability appears to be the main reason for illegal migration movement throughout the world. Nevertheless, many of the willing migrants undertake the hazardous travel to their destination country with criminal organisations specialized in people smuggling and arrange everything for the migrants, but at a high price. Very often the traveling conditions are inhumane: the migrants are overcrowded in trucks or boats and fatal accidents occur frequently. After their arrival in the destination country, their illegal status puts them at the mercy of their smugglers, which often force the migrants to work for years in the illegal labour market to pay off the debts incurred as a result of their transportation.

A number of recent examples highlighted by the UN and ILO serve to illustrate the horrors of these crimes. Police in Nigeria freed 32 teenage girls from a so called "baby factory" used to feed the region's expanding sex trade and human trafficking markets. The police in the southern Nigerian city of Aba raided the clinic, known as The Cross Foundation, after receiving a tip that the owner was harboring pregnant girls and selling their babies. Some of the girls, who were between 15 and 17, told authorities that the clinic's owner, Dr. Hyacinth Orikara, forced them to sell their babies to him for around US\$190, depending on the gender. The organisations sell newborns to the highest bidder and the children often end up being used as factory workers, mine workers or sex slaves.

In 2005, 5 criminals of Turkish origin were arrested and in 2006 convicted in the UK in relation to illegal smuggling of mainly Turkish migrants, sentenced to lengthy prison sentences and receiving confiscation orders totalling over £25mio. The illegal immigrants were predominantly Turkish and were smuggled into the UK by lorry as well as motor vehicle, trains and light aircrafts. The fee charged per immigrant was believed to be in the region of £3,500 for a channel crossing and up to €14,500 from Turkey across Europe. This money would cover the transport cost, the cost of the documentation, which is needed in the UK, although this documentation was usually false. The money would also cover the cost of accommodation on arrival in the UK. It is estimated that over 20,000 immigrants were smuggled into

the UK by this group of individuals. Interpol have taken a lead particularly in Africa with numerous operations focussing on child labour trafficked in the region. For more details see Part 2, Section 7, Human Trafficking. A case of child sexual exploitation also caught by Interpol in Holland is that of Robert Mikelsons who was identified as part of a paedophile ring.

A large proportion of the funds generated by Human traffickers will be in cash. These criminal proceeds will be used, depending upon the type of trafficking involved to offset expenses incurred in the operation. Cash may be generated in one currency and in one location and expenses incurred in one or more different currencies and/or one or more different countries and so Money Services Businesses may be used by the Human Traffickers. In order to launder the net cash proceeds of human trafficking, cash intensive businesses may be used. In one case in the UK, Turkish Kebab shops were first acquired (for cash) and then used to launder net cash proceeds in the UK. Use of legitimate cash generating businesses like Kebab shops, but also takeaway outlets, snooker halls etc were also used to launder criminal funds. The money generated through these company accounts was in excess of the funds generated by comparable businesses.

Human Trafficking by Organised Criminal Gangs may use alternative cash intensive businesses, for example, saunas and massage parlours, bars and nightclubs and casinos have been used to both launder cash and as venues for the offering of prostitution services. Chinese Triads may utilise Chinese laundry services and Italian Mafia and the Italian American Mafia may similarly utilise Italian restaurants. Individual bank accounts may be opened and utilised though human traffickers will want to avoid large concentrations of cash deposits into single accounts and repeat wires, particularly offshore which could raise suspicions. Use of multiple accounts and credit cards from various financial institutions may therefore be used with the effect that turnover is diluted. Use of associates, family members and use of alias identities, may also be used to open and operate accounts, also use of front companies. Human traffickers are often well connected with those able to forge identification documents.

Illicit Arms Trafficking

About 526,000 people lose their lives every year due to armed violence, which is commonly fuelled by illicit weapons. That is the equivalent of one person dying violently every minute.

UN August 30, 2012 press release DC/338⁷

Harms

When weapons are smuggled into a country and sold illegally, government regulations to identify buyers and license users don't apply, which makes it easier for criminals to obtain weapons. The black market for arms can include tanks, radar systems that detect Stealth aircraft, and components for weapons of mass destruction. However, small arms transfers fuel crime and sustain armed conflicts worldwide, from Afghanistan to Liberia to Colombia. Regions plagued with state conflict and ethnic and religious disputes stoke demand for small arms. Terrorist Groups rely on the black market for arms supplies. An inexpensive shoulder-fired surface-to-air missile can destroy a commercial airliner.

"Armed conflict, often fuelled by illicit weapons, destroys communities and extinguishes any hope of eliminating poverty for millions of people," said Stan Nkwain, Chief of Policy and Planning at the UN Development Programme's Bureau for Crisis Prevention and Recovery. "When these weapons fall into the hands of criminals, combatants and terrorists, they destroy economic stability, undermine the rule of law and subvert legitimate Governments," he added. "Also, armed violence and violence against women are tragically interlinked, as having weapons in the hands of abusers increases the risk of domestic violence." UN August 30, 2012 press release DC/338⁷.

Statistics

According to the Small Arms Survey,³ authorized transfers of small arms and light weapons, their parts and accessories totalled at least US\$8.5bio in 2012 or more than double the previous estimate in 2006, with ammunition accounting for half that amount.

The Survey also reported that there are an estimated 875 million small arms in circulation worldwide, produced by more than 1,000 companies from nearly 100 countries.

The upsurge in procurement was as a result of the conflicts in Afghanistan and Iraq, and the arming of State actors. Additionally, civilian procurement in the US as well as greater transparency were credited with

reasons for the increases.

Despite improvements in transparency, few countries scored well focussing on just such a measure. From 54 countries examined in 2013, judging them on a 25-point scale. Switzerland had been the most transparent, followed by Germany, Romania, Serbia, Netherlands and the UK and at the other end of the scale, Iran, North Korea, Saudi Arabia and UAE had been the least transparent, scoring zero. China and the Russian Federation, both importers as well as exporters, were also in the bottom 15.

Transparency Barometer	
1	Switzerland
2	Germany
3	Romania
4	Serbia
5	Netherlands
6	UK
50	South Africa
51	Iran
52	North Korea
53	Saudi Arabia
54	UAE

Source: Small Arms Survey 2013⁴

For some of the least transparent countries they might not produce weapons, but they re-exported and re-transferred them. Looking at the top exporters, the US had topped the list of 12 countries exporting at least \$100 million worth of small arms and light weapons. Two of them, France and Japan, had reached that figure for the first time, while Italy, Germany and Brazil had also ranked high.

Whilst there is increasing transparency and an understanding of still the dangers of the trade in licit weapons, the trade in illicit weapons remains a matter of grave concern. According to the head of the Small Arms Survey, Mr. Berman claimed that the combined figure for licit and illicit trade could be more than US\$10bio, placing the estimate of illicit arms at approx US\$1.5bio.

Whilst it is often assumed that the illicit arms trade causes most concern in nascent war zones fueling violence, it is in non-convict or war zones where the most damage is inflicted. Countries such as El Salvador,

Jamaica, and South Africa suffer from extremely high recorded levels of murder's with more deaths each year than in many contemporary wars.

Non-conflict deaths are often distinguished from the deaths that arise from armed conflict based on the organisation of the killing. Homicide is usually committed by individuals or small groups, whereas the killing in armed conflict is committed by relatively cohesive groups of up to several hundred members. But there is often little difference in intensity between large-scale criminal violence and low-level armed conflict, and the line between the two is frequently blurred.

Approximately 60% of all violent deaths are committed with firearms, with variation from a low of 19% in West and Central Europe to a high of 77% in Central America, based on data from 45 countries. That represents 245,000 firearms deaths per year.

Non-conflict armed violence includes murders, suicides, extra judicial killings, and other forms of death or injury, such as those resulting from domestic violence or gender-based armed violence, social cleansing, or disappearances and kidnappings.

Definition/Description

Arms trafficking, also known as smuggling or gunrunning, is the illegal transfer of contraband weapons or ammunition. What constitutes legal arms trade depends on which of a wide variety of laws apply.

While there is no universal definition of small arms or light weapons, a widely adopted definition is that proposed by the 1997 Report of the UN Panel of Governmental Experts on Small Arms. The Panel's list is organised into "small arms" and "light weapons": "small arms": revolvers and self-loading pistols, rifles and carbines, assault rifles, sub-machine guns and light machine guns and light weapons: heavy machine guns, hand-held under-barrel and mounted grenade launchers, portable anti-aircraft guns, portable anti-tank guns, recoilless rifles, portable launchers of anti-tank missile and rocket systems; portable launchers of anti-aircraft missile systems (MANPADS); and mortars of calibres of less than 100mm.⁵

Small arms are for personal use, and light weapons are for use by a unit of persons. Ammunition and explosives also form an integral part of small arms and light weapons used in conflict.

Whilst in 2005 a Protocol against the Illicit Manufacturing and Trafficking in Firearms, their parts and components and Ammunition (Palermo

Protocol) was issued, supplementing the Convention against Transnational Crime in 2000 which focussed on illicit arms trafficking encouraging parties to the protocol to adopt and implement the strongest possible legislation to investigate and prosecute those found guilty of illicit arms trafficking, UN Member States failed in 2012 to negotiate a more comprehensive Arms Trade Treaty to establish standards for international trade in conventional weapons. However, in August of 2012, the UN launched "International Small Arms Control" to monitor Member States' implementation of the programme they had agreed to in 2001 – the 'Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects.' The programme focused on making illicit gun manufacturing a criminal act, destroying surplus supplies of weapons, and creating processes for identifying and tracking weapons.

Finally in 2013 the UN Arms Trade Treaty was adopted which provides for common international standards for the import and export and transfer of conventional arms.

Some bilateral government initiatives focus on hot spots for trafficking. For example, the US-Mexico Mérida Initiative was launched to disrupt the flow of firearms, ammunition, explosives and bulk cash being trafficked/smuggled from the US into Mexico. US and Mexican agencies are sharing a web-based system which allows investigators to trace weapons known to originate from the US. On the supply side, the US is taking more steps to secure and destroy excess weapons stockpiles and to mark weapons with traceable identifiers. Strategies to disrupt the operation of these smuggling rings include training and coordination in investigations, prosecutions, and bulk cash seizures.

But in general, effective multilateral frameworks to combat arms trafficking are not yet in existence, and this fact benefits traffickers. Dealers hopping from one jurisdiction to another can take advantage of inconsistent legal requirements.

Black market arms dealers don't usually identify themselves as such. For example, arms trafficker Viktor Bout, identified himself as being in the transport business. Traffickers tend to move before establishing a reputation, and gravitate towards countries with either few regulations, ample opportunities for corruption or good transport and logistical support. Viktor Bout for example, used one of the lesser known Emirates of the UAE, Sharjah as have others.

Historical Background/Content

Since the end of the Second World War, tens of millions of people have been killed by conventional weapons, mostly small arms such as rifles, machine guns and rocket-propelled grenade launchers. Sales of advanced weaponry, fighter jets and high-tech electronics, sophisticated long-range artillery and warships, and "weapons of mass destruction" tend to receive the most press coverage. But these costly, sophisticated weapons have not proved as deadly as ordinary guns and grenades that are easy to buy, easy to ship and easy to use.

Low-tech, handheld weapons and explosives do the vast majority of the killing today. There are more than 550 million small arms currently in circulation, many of them fueled bloody civil strife in countries from Angola to Afghanistan, Colombia to the Congo Sri Lanka to Sierra Leone and Somalia to Sudan and in many more.

In most cases, the countries involved in these conflicts have been the subject of international embargoes imposed by the UN and other organisations. In some cases, major powers want to supply the side they favor in the conflict but do not want their "fingerprints" to be discovered on weapons of war, with the recent struggles in Libya and in Syria being good examples.

Against this backdrop of embargoes and clandestine international politics, a specialized group of arms dealers emerged during the Cold War. Their role was to ensure that responsibility for the death and destruction could not be traced directly to the supplier and they pocketed millions for themselves in the process.

The richest and longest-lived practitioners of this business simply "fronted" for a particular government or alliance or even "ruling family." In the 1950s and 60s, the late legendary Sam Cummings, a CIA veteran, supplied anyone who had US government approval with weapons from stockpiles in the US and the UK. And, of course, there were the "middlemen" such as Adnan Khashoggi, who in the 1970s and 80s often fronted for the interests of the Saudi royal family, whilst acting as a commission generating Intermediary for US Arms companies.

But it is not only individuals who operated in the clandestine international arms market. In some instances, countries that were subject to embargoes also got into the clandestine weapons business. Israel, apartheid-era South Africa and Taiwan are examples of countries compelled to develop their own arms industries and to seek to circumvent international trade bans against them.

During the first 25 years of its existence, Israel was often denied weapons and ammunition by US and European governments, as well as most nations in Asia and, of course, the Middle East. As a result, it built its own arsenal and related industries that are to this day active internationally. Israeli arms and trainers have turned up in China, Guatemala, Ecuador and Central Africa. Israel Defence Industries has a long history of both procurement and development of military technology and its sale overseas. The man once known as the richest Israeli, the late Shaul Eisenberg, is an example of the "legitimate" arms entrepreneur using the trade in weapons and weapons technology to create a multi-faceted business empire.

Money Laundering

It is the role of the clandestine middleman, the so called "Lords of War" or "Merchants of Death" that have made their marks in indelible ink over more than 50 years helping dictators bent on genocide and rebels relishing revolution spill the blood of millions that is of greatest concern. Often, they are the key players who provide the deniability that the government supplying the weapons seek. They can all trace their steps back to the "super salesman of death", the "mystery man of Europe" the "Monte Cristo of our Time", Basil Zaharoff who was at the turn of the last century, the worlds first flamboyant larger than life arms dealer, a man who once boasted of starting wars in Africa so he could sell weapons to both sides, who helped arm the great powers culminating in the First World War! his greatest achievement and as a result of his success, many have since attempted to emulate.

Each are largely motivated by money but the consequences of their actions can be staggering irrespective of the monies earned. As Henry Ford famously stated, "show me who makes a profit from war, and I'll show you how to stop a war".

Some of the most successful individuals making most out of war in the twentieth century include: Sam Cummings and Adnan Khashoggi, the list of shame includes: Dale Stoffel; Dr. Moosa Bin Shamsher; Fares Mana'a; Sarkis Soghanalian; Monzer al-Kassar; Pierre Falcone and his partner; Arcady Gaydamak; Jean-Bernard Lasnaud; Leonid Minin; Tomislav Damnjanovic; Simon Mann; Andrew Wang (see Thomson CSF-Thales) and Viktor Bout and many more.

Insider Dealing

"The public's out there throwing darts at a board, kid. I don't throw darts at a board; I bet on sure things,"

so said Gordon Gekko in Oliver Stone's

1980s-defining film "Wall Street." With those words, the "greed is good" trader, largely based on Ivan Boesky, explained to his young protégé how inside information can turn investment into a one-way bet.¹

Introduction

Whilst individuals are generally entitled to trade in the securities of the corporations with which they are involved or to trade in other securities without restriction, such trading becomes illegal Insider Dealing when privileged, non-public, material information is used by an individual to buy or sell a security or to tip someone else off who may trade.

Harms

Insider trading is both a theft and a financial Fraud. The victims are all those market participants that play by the rules, investing based on publicly available information and dealing honestly. The abuser, when he trades on inside information cheats every other participant and offends the principles of the Markets that honest participants rely upon.

Illegal insider trading is also believed to raise the cost of capital for securities issuers, thus decreasing overall economic growth.

According to US Attorney Preet Bharara in a widely reported October 20, 2010 speech to the New York Bar Association,² illegal insider trading is rampant and may even be on the rise, with some cheating the system including not only some at Wall Street firms, but also at Main Street companies. Bharara made the point that many of the people who are going to such lengths to obtain inside information for a trading advantage are already among the most advantaged, privileged, and wealthy insiders in modern finance. Widely quoted Bharara then stated that "But for them, material non-public information is akin to a performance-enhancing drug that provides the illegal "edge" to outpace their rivals and make even more money. In some respects, inside information is a form of financial steroid. It is unfair; it is offensive; it is unlawful; and it puts a black mark on the entire enterprise."

Some however take a different view. For example Milton Friedman argues that laws making insider trading illegal should be revoked, claiming that insider trading based on material non-public information

benefits investors, in general, by more quickly introducing new information into the market. He stated that, "You want more insider trading, not less. You want to give the people most likely to have knowledge about deficiencies of the company an incentive to make the public aware of that." Friedman did not believe that the trader should be required to make his trade known to the public, because the buying or selling pressure itself is information for the market. Other critics argue that insider trading is a victimless act: A willing buyer and a willing seller agree to trade property which the seller rightfully owns, with no prior contract (according to this view) having been made between the parties to refrain from trading if there is asymmetric information. The Atlantic has described the process as "arguably the closest thing that modern finance has to a victimless crime".

Statistics

The UK FSA reported in 2005³ that they had looked into market cleanliness by reviewing the extent to which share prices moved ahead of significant, potentially price sensitive, regulatory announcements that companies are required to make to the market. This analysis was conducted for two types of statements - trading statements made by FTSE 350 issuers and public takeover announcements related to UK companies.

The figures for FTSE 350 issuers showed a marked improvement in the level of untoward activity down from 19.6% in the period 1998-2000, to 11.1% in 2002/03 to only 2.0% in 2004/05. However, the figures for takeover announcements were 32.4% in 2004 to 24% in 2000. The latest figures for 2005 were 23.7%. This led the UK regulator to conclude that nearly a quarter of all UK mergers and acquisitions in 2005 involved "informed trading". The regulator admitted that the level of suspect trading is "higher than we would expect in a clean market. The regulator believes that the risk of leakage is heightened by the way transactions are conducted and the number of people involved in the process. For example, in a recent investigation FSA were provided with an insiders list of over two thousand names. Lists, and indeed the transactions to which they relate, often include multiple parties and numerous advisors; this inevitably increases the risk of information leakage.

Figures collated by Thomson Financial in 2007 for a UK newspaper, also pointed to the widespread likelihood of illegal pre-takeover trading. They showed that the share prices of several of the UK's biggest takeovers moved materially ahead of the announcement of bid talks. For example, George Wimpey's shares rose by 18p to 653p on the announcement that it was merging with Taylor

Woodrow. The shares had already risen from 540p on March 14, however. ICI, which jumped from 549p to 634.5p on 18 June after Akzo Nobel said it was looking at buying the former bellwether stock, had already risen from 506.75p in only five trading sessions.

A study by Measuredmarkets Inc. in August 2007⁴ in the USA showed that insiders may have traded illegally in advance of 41% of the largest US acquisitions the previous year. Two months later, Credit Derivatives Research LLC found⁵ that credit-default swaps based on the bonds of 30 takeover targets, including four of the five biggest leveraged buyouts by that point in 2006, rose before deals were announced.

Also in 2007 it was reported that, trading in options to buy shares of TXU Corp. surged more than seven-fold before CNBC said the company would be acquired in the largest-ever leveraged buyout and the volume of options trading to buy shares of Hyperion Solutions Corp. rose almost six-fold before Oracle Corp. said it would buy the company for US\$3.3bio.

The demand for performance among hedge funds where a percentage point in performance can mean the difference in millions of dollars of additional compensation based on pre agreed performance fees is a clear risk factor. In the US there are more than 9000 hedge funds in operation today, managing US\$1.4 trillion, with some estimates placing assets as high as US\$2.3 trillion, plus 6 to 1 leverage. About a thousand of these same hedge funds go out of business every year, with a 1000 new start-ups coming on stream. The incentive for some to engage in Insider Dealing is obvious.

Definition / Description

Today, insider dealing and market abuse are largely accepted as requiring both criminal and administrative sanctions. The international framework has been shaped by the anti trust and securities reforms initiated in the US and largely adopted as common principles throughout the world where Markets for Financial Instruments are found.

It wasn't until the 1980s that insider dealing would really hit the headlines, when major prosecutions grabbed the media's attention and later many countries then started to criminalise insider dealing. Whilst the US relies on broad anti-fraud provisions contained in the federal securities laws, e.g., Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5, the EU and much elsewhere in the world relies on a specific statute, though in practice the laws are similar. Whilst the EU passed insider dealing laws in 1989, following

13 years of discussion. Notwithstanding criminalization, it would still take another 20 years before many including the UK and others in Europe began to make insider dealing prosecutions a priority.

Insider Dealing

Generally speaking, insider trading is when a corporate insider trades in the securities of his or her corporation on the basis of material non-public information. In the US the so called "classical" theory of insider trading targets a corporate insider's breach of duty to shareholders with whom the insider transacts. The more recent US "misappropriation" theory prohibits trading on the basis of non-public information by a corporate outsider in breach of a duty owed not to a trading party (i.e., the shareholders of the company), but rather to the source from which the trader learned the information.

Tipping Off

Insider Dealing liability can also apply to "Tipping off" someone who makes a trade, so that even if a person does not make a trade himself, if he shares non-public information with someone who makes a trade based on his information, both he and the person who actually makes the trade can be guilty of insider dealing.

Misuse of Information

A related malpractice is the "Misuse of Information," where for example a customer of a financial services firm places an order for a large block of stock, whether buy or sell, this information is proprietary to the customer and should be kept confidential by the broker involved. Nevertheless, individuals with knowledge can trade ahead or at the same time, personally benefitting. Such trading is normally in breach of applicable law and/or regulations and is known as Front and or Parallel Running (see below for details).

FATF have included insider dealing alongside market manipulation as a predicate offence for money laundering in their 40 Recommendations.

United States

The US has relied largely on its courts to develop the law prohibiting insider trading and market abuse. Whilst a form of insider dealing conviction was obtained in 1909 when the US Supreme Court in *Strong V Rapide* held that a company official was obliged to disclose his identity and non-public information when he trades his stock, it wasn't until after the US stock market crash of 1929 that brought the Securities Act of 1933 and the Securities Exchange Act of 1934, aimed at controlling the abuses believed to have contributed to the crash, that a statutory response was codified. The 1934 Act addressed insider trading

directly and indirectly and has been supplemented by later SEC rulemaking and case law. For example, whilst the Securities Act S.17(a)(1) prohibited fraud and misstatements in the sale of securities, there was no comparable provision prohibiting such practices in connection with the purchase of securities. In 1942, the SEC remedied this oversight adding the words ‘in connection with the purchase or sale of any security’ and promulgated Rule 10b-5 which then read: It shall be unlawful for any person, directly or indirectly . . . , (a) to employ any device, scheme, or artifice to defraud, (b) to make any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading, or (c) to engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of a security. These broad anti-fraud provisions make it unlawful to engage in fraud or misrepresentation in connection with the purchase or sale of a security and therefore cover both insider dealing and market manipulation. In the more than 50 years since its adoption, this simple rule has been involved in countless SEC and private proceedings, and applied to almost every conceivable kind of situation. In the 1960s and early 1970s, many federal appellate courts and district courts developed expansive interpretations of Rule 10b-5 (and other antifraud provisions of the securities laws). One of the first cases that established the modern insider dealing offenses was that of *Cady Roberts & Co* 1961. Increasingly liability for negligent as well as deliberate misrepresentations, for breaches of fiduciary duty by corporate management were imposed and for failure by directors, underwriters, accountants and lawyers to prevent wrongdoing by others.⁶ Further ad hoc rule making has continued for example, in 2000, the SEC enacted Rule 10b5-1, which defined trading “on the basis of” inside information as any time a person trades while aware of material non-public information - so that it is no defence for one to say that she would have made the trade anyway. This rule also created an affirmative defence for pre-planned trades.

United Kingdom

Insider dealing has been a criminal offence in the UK since 1980. Steps to introduce legislation took a number of years. Up to the end of World War II the buying and selling of stocks and shares in a company on the basis of information known only to the company or its directors, officers and advisors was considered legitimate and widespread. Between the end of the World War II and the late 1950s it began to be considered unethical to make private profits at the expense of the main body of shareholders but in the 1960s and early 1970s the

practice became widespread once more, often using knowledge of a take over. Insider dealing was even described by the Financial Editor of the Sunday Times in 1973 as the “crime of being something in the City”.⁶ In 1973 The Stock Exchange and the Takeover Panel issued a joint statement calling for criminal sanctions. A number of subsequent attempts to pass legislation through Parliament failed, but in 1980 Part V of the Companies Act 1980 came into force and made insider dealing a criminal offence in certain circumstances. These provisions were subsequently consolidated as the Company Securities (Insider Dealing) Act 1985, and amended by the Financial Services Act 1986. The impetus for further reform then came from within the European Community when in 1989, the Council of the EC agreed on a Directive to co-ordinate regulations on insider dealing (see below). In the UK, the relevant law implementing the EU Insider dealing Directive is The Criminal Justice Act 1993 Part V. In the case of Market Abuse it took until 2000 and the passing of The Financial Services and Markets Act 2000, which defines an offence of Market Abuse and was followed by the FSA’s Code of Market Conduct which sets out in detail the standards that should be observed by everyone who uses the UK’s key financial markets, whether they are trading in the UK or from overseas.

Section 118 of the Financial Services and Markets Act 2000 (FSMA), remains and now incorporates existing EU MAD legislation, i.e. the EU Market Abuse Directive (MAD) which came into force in July 2005. The MAD provisions were similar to those in a number of existing EU countries, in particular in the UK. The UK FSA issued a Code of Market Conduct⁷ (August 2009)⁸ which runs to 52 pages and covers seven market abuses spanning- i) insider dealing, ii) improper disclosure, iii) misuse of information, iv) manipulating transactions, v) manipulating and “fictitious” devices, vi) dissemination of information, and vii) misleading behaviour and distortion. For more information see the UK FSA Code of Market Conduct (issued August 2009).

European Union

In the European Community it wasn’t until 1989 that the EC agreed on a Directive to co-ordinate regulations on insider dealing. The EC Directive was thirteen years in the making; the first deliberations beginning in 1976. The Directive was modelled on French and English insider trading prohibitions. At the time the Directive was passed, four of the 12 members of the EC - West Germany, Belgium, Italy and Ireland - had no insider trading legislation on the books and the remaining eight members - France, England, Luxembourg, the Netherlands, Denmark, Greece, Portugal and Spain -

had widely varying statutes. Several of the members took time well beyond the 1992 deadline to get legislation in place. Luxembourg, for example, enacted its version of the Directive in 1997. The Directive defines “inside information” as information of a “precise nature” about security or issuer which has not been made public which, if it were made public, “would likely have a significant effect on the price” of the security (Article 1); It prohibits insiders from taking advantage of inside information (Article 2); It prohibits insiders from tipping or using others to take advantage of inside information (Article 3); It applies its prohibitions to tippers with “full knowledge of the facts” (Article 4); It requires each member to apply the prohibitions to actions taken within its territory with regard to securities traded on any members’ market (Article 5); It provides that members may enact laws more stringent than set out in the Directive (Article 6); It requires issuers to inform the public as soon as possible of major events that may affect the price of the issuer’s securities (Article 7); It requires members to designate an enforcement authority, to give it appropriate powers and to bind it to professional standards of confidentiality (Articles 8 and 9); It requires members to cooperate with each other in investigation efforts by exchanging information (Article 10); It leaves it up to individual members to decide on penalties for insider trading (Article 13); and finally, It required all members to enact legislation complying with the Directive by June 1, 1992. A fundamental difference between the EC Directive and the US’ prohibition against insider trading under Section 10b and Rule 10b-5 as developed by the courts, is that the Directive does not require that the insider trader breach a fiduciary duty to the source of the information for liability to attach. In this respect, it mirrors the US’ prohibition against trading on the basis of non-public information about a tender offer under Section 14(e) of the Securities Exchange Act of 1934 and the Commission’s Rule 14e-3.

International Securities Regulation

The leading body active in this field is the International Organisation of Securities Commissions (IOSCO) who published in 1998 The “Objectives and Principles of Securities Regulation”⁹ updating these in 2003 stating amongst other things that “Investors should be protected from misleading, manipulative or fraudulent practices, including insider trading, front running or trading ahead of customers and the misuse of client assets.” More than 85% of the world’s securities and commodities market regulators are members of IOSCO and have signed on to these Core Principles. The World Bank and International Monetary Fund now use the IOSCO Principles in reviewing the financial health of different country’s regulatory systems as part of these

organisations’ financial sector assessment programme, so laws against insider trading based on non-public information and misleading, manipulative or fraudulent practices are now expected by the international community. Enforcement however varies widely from country to country, but the vast majority of jurisdictions now outlaw these practices, at least in principle.

Switzerland

Under pressure to step up the battle against insider trading. Insider trading only became a crime in Switzerland in 1988, but the law was written far more narrowly than in other countries. Unlike the UK or the US, insider trading was an offense only in relation to the issue of new securities, mergers and acquisitions, but not ahead of earnings announcements, even when they contained potentially market-moving information. Moreover, Swiss law didn’t require mandatory jail time, and the fines were considered low by some politicians and regulators to be an effective deterrent. According to FINMA Circular 2008/38 – Market Conduct Rules,¹⁰ “Securities trading is to be based upon generally available or published information on securities and issuers or upon information derived therefrom. Information on securities and issuers is deemed generally available when it is published or disseminated in the media or via the usual information channels in the financial sector, or if it is derived from such information. All other information on securities and issuers is to be regarded as confidential. Misusing knowledge of confidential price-sensitive information for securities transactions is not permissible (misuse of information). Information is deemed price-sensitive where it is capable of significantly influencing the stock market price or the valuation of the respective securities. Specifically, such information pertains to circumstances that substantially impact a company’s organisational structure, its executive and business management bodies, its course of business, its financial or earnings situation and thus its valuation, and is therefore capable of effecting material changes in the market price. These circumstances may be grounds for public disclosure and/or be subject to legal or self regulatory requirements to provide information (disclosure obligations pursuant to Art. 20 SESTA or ad-hoc publicity according to stock exchange regulations). The wrongful dissemination of confidential price-sensitive information or making references or recommendations based thereon pertaining to engaging in securities transactions are also deemed to constitute misuse of information. Rumours or vague hints are not deemed confidential information. However, knowingly spreading rumours or vague hints for the purpose of invoking same is not permissible. Taking advantage of the expected market reaction of market participants and of securities prices employing

the knowledge of an impending announcement of investment recommendations ("scalping") is not permissible

Looking ahead, a further tightening of laws on Market Abuse is expected with for example, the EU MAD 2 regime, new Swiss insider dealing laws and new provisions within Dodd Frank in the US, all either recently in force or to have effects in the years to come. For more details see Part 1, Section 3, Money Laundering Laws & Regulations below.

Regulatory Expectations on Financial Institutions

According to the UK FSA "All financial services firms are responsible for ensuring that their employees are vigilant in preventing market abuse. In doing so, firms should look to determine: (i) That all staff have been adequately trained and understand what constitutes market abuse; (ii) That market abuse controls stand up to increased scrutiny from the regulator. In particular, whether: a) Conflicts of interest controls pass a thematic regulatory review; b) Confidential and price-sensitive information remain secure; c) Risk-based compliance monitoring programmes are frequently reviewed; and d) Whether current management information effectively alerts senior management to potential problems; e) Whether recent market troubles have increased the occurrence, opportunity or discovery of market abuse; and f) Whether the compliance department is adequately staffed to ensure resource is not diverted away from monitoring or tackling market abuse.

In a speech given by Margaret Cole, then Director of Enforcement at the UK FSA in 2007 she stated that,"We firmly believe that prevention is better than cure and to this end we have made it clear to market participants that we expect proper conduct including: appropriate and effective systems and controls in form of robust internal procedures; an insider list that is short as possible and based on need-to-know; a willingness to undertake a thorough internal review following a leak; effective and targeted training of staff including support staff; monitoring of staff personal account dealing; robust controls when dealing with third parties; effective information technology controls; and an awareness of the limitation of code words as an effective tool to keep information confidential, especially if used in isolation."

In the US, the New York Fed has stated that it has general expectations of good practice as follows: "Trading desk management and the supervision, legal, and compliance staff should work collectively to ensure that any questionable trading practices are identified and addressed in a timely manner. Trading desk management and supervision should be aware of, and responsible for, strategies executed by the trading

desk. Other control functions, and particularly legal and compliance staff, should be poised to promptly evaluate and respond to questionable trading practices should they occur. Firms should aspire to provide system tools that relay real-time trade position information to the compliance function in order to provide timely notification of large positions."

From pronouncements and speeches made, key areas of increased concern include, high frequency trading, the size of insider lists, low value securities, (so called "Penny Stocks"), options and futures markets, energy and commodities markets, dark pools and MTFs, hedge funds customer insiders and expert networks as well of course of classic manipulative practices (see Market Manipulation below) manipulative rate fixing and collusive and anti competitive practices.

Historical Background / Content

For many years governments on both sides of the Atlantic (and now in APAC and elsewhere) relied on markets to drive economic growth and political influence and despite obvious abuses, were loath to interfere in the so called free markets, afraid of stifling their development. There are many hundreds, if not thousands of examples through the years of significant abuses perpetrated on market participants, including investors, that have unfairly disadvantaged the abused and undermined the integrity of the markets involved but only a few have led to increased governmental intervention to regulate free markets.

The history of market abuse is interwoven and inseparable from the history of markets themselves, both in their advances and in their reversals. In many cases it is the publicised abuses themselves and their proponents that both triggered and accelerated many of the most significant market reversals and these consequences that eventually encouraged legislators and judges to shape today's legal and regulatory frameworks and institutions responding towards Market Abuse. The staggering success of the Dutch East India Company, listed on the very first Stock exchange in Amsterdam and lasting 200 years returning an average annual dividend of 18% is a shining example of the power and utility of Markets, whereas the British South Sea Company, which led to the South Sea Bubble in 1720 and a calamity in England is a shining example of what can happen when things go badly wrong with Markets. There are many more examples of both great companies and investments, of great entrepreneurs and robber barons, of captains of industry and crooks that illuminate the story of the development of Markets and highlight the constant attempts to abuse them for personal gain. Whilst booming Markets followed by occasional Panics

and Crashes were the norm throughout the Eighteenth and Nineteenth century it was not until the Twentieth Century, that the laissez faire attitude towards Markets and their regulation began to change and a new way forward proposed. The new way was pioneered in the US, which until then had taken a staunchly free market approach. It would take until the end of the so called first Gilded Age or the end of the reign of the Robber Barons beyond the turn of the Twentieth Century, before a backlash against Market Abuse would be seen. This did not equate to a backlash against Markets per se, which had largely been credited with the emergence of the US as the worlds foremost industrial superpower. The backlash focussed first though on monopolistic corporations being confronted with the enactment and use of The Sherman Anti Trust Act of 1890, the implosion of Charles Ponzi's pyramid scheme in 1923 and then the bursting of the Florida Real Estate Bubble and Crash in 1926 which was a foretaste of something much bigger, the Stock Market Crash of 1929 and the Great Depression that followed, affecting both rich and poor, which led to the Securities Market Reforms (1933 & 1934) and the establishment of the SEC as part of America's New Deal."

For the next 40 years or so, negative headlines would largely be grabbed by ad hoc unexpected accounting frauds, for example McKeeson & Robbins in 1937 which led to the tightening in external audit procedures and ZZZZZ Best which relied on phantom contracts and sales figures to mislead investors. The Insider Dealing offence in the US would be developed through prosecutions, each time the offence would become more broadly interpreted, for example in 1961 in Cady, Roberts & Co and in the early 1980s in Chiarella, Newman and Dirks and then with the prosecution and conviction of R Foster Winans the co writer of the WSJ's "The Heard on the Street" who leaked advance word of the contents of this widely followed stock picking publication.

The mid 1980s would bring the story into the modern age. With deregulation, markets prospered and capital flowed more easily and with the rise of leverage, including the availability of junk bonds for financing, a mergers and acquisitions boom was unleashed. Insider dealing would take centre stage in 1985 with the arrest of Ivan Boesky, (Gordon Gekko), being followed by a string of others including Ernest Saunders and the Guinness Gang of Four in the UK and the prosecution of "Junk Bond King" Michael Milken and the fall of Drexel Burnham Lambert. Many countries then took the opportunity to criminalise insider dealing following the US and latterly the UK's lead, though it would still take another 20 years before many including the

UK began to make insider dealing prosecutions a real priority. In 1987 following a bull market run of over 5 years US Markets turned on 19 October 1987, a date that subsequently became known as "Black Monday," which was the greatest loss Wall Street had ever suffered on a single day. Nevertheless, by September 1989, the market had regained all of the value it had lost in the '87 crash.

The 1990s followed the passing of EU wide laws on insider dealing in 1989, following 13 years of discussion. More prosecutions for insider dealing in the US continued but none with the profile of the previous decade. A major market manipulation scandal at Salomon Brothers in 1991 in New York forced the toppling of their legendary CEO, John Gutfreund (of Liar's Poker fame) and the firm was saved from probable extinction by the even more legendary Warren Buffet. From the middle of the decade, we would see the start of the dot-coms. By October 1999, the six biggest tech stocks of that time - Microsoft, Intel, IBM, Cisco, Lucent and Dell - boasted a combined value of US\$1.65 trillion, or 20% of the US gross domestic product (GDP). Whilst these great companies prospered, most did not. In 1998, internet community site Globe.com had set a record with an IPO that sky-rocketed 606% on its first day of trading, but like many others, it would run out of initial capital and quickly go bust. The subsequent demise of the dot-coms triggered a panic with the bubble bursting on 10 March 2000. By the end of 2000 the NASDAQ slid to 2471 from the March peak of 5048.

The bursting of the bubble, brought Eliot Spitzer, the NY District Attorney to the fore, crusading first against research analysts at Merrill Lynch, principally Henry Blodget, and then others including Jack Grubman at Salomon Smith Barney, part of Citigroup, alleging fraud in continuously supporting dot-com companies publicly while privately having grave concerns over their prospects or viability. Spitzer's investigation would lead to wholesale changes, cleaning up research practices and conflicts of interest across all of Wall Street. For details see the Global Analyst Research Settlement in Part 2, Section 8. Spitzer would then turn his attention to late trading and market timing malpractices first on Edward Stern and Canary Capital, but in time to others including Bank of America, Bank One, Janus and Strong Capital Management and in doing so he would have a similar effect on the US Mutual Fund Industry as he did on the Investment Banking Industry. For details see the Mutual Fund Scandal in Part 2, Section 8.

The bursting of the bubble and the resulting economic downturn coincided with the demise of some leading

businesses, including Enron and then soon followed WorldCom, each the then largest corporate failures in history, with others Tyco, Global Crossing, Qwest, Adelphia, HealthSouth and in Italy, Parmalat - all guilty of massive accounting fraud. In the case of Enron, its failure was preceded by both insider dealing in the Executive Suite and by criminal market manipulation of the California electricity markets which led to the California Electricity Crises in 2000 / 2001. Enron would also take its auditors, Arthur Anderson down with it. To address these scandals Sarbanes Oxley in the US was passed in 2002 to strengthen accountability of auditors, top executives and boards.

Also in the early part of this decade the SEC adopted Regulation FD and Rule 10b5-1, requiring Companies not to make selective disclosures and further tightening restrictions on insider dealing but also providing a safe harbour for pre planned trades.

During this decade insider dealing was joined by offences relating to manipulating markets in many parts of the world and whilst actions against manipulators would still lag behind insider dealing cases these picked up and both insider dealing and market manipulation became the focus of regulators worldwide with regular prosecutions of both individuals but also firms, record terms of imprisonment being secured, penalties and record fines being levied. Cases such as Martha Stewart, Shell, George Soros, Citigroup with their programme trade known as Dr Evil in Europe, Insider Rings, Livedoor in Japan and many others made regular headlines.

With the onset of the Financial Crises in 2007, headlines were dominated by Bear Stearns, then Lehman Brothers, toppling Enron and then WorldCom as the world's largest ever bankruptcy and the frauds at the heart of the US real estate mortgage markets. Bernard Madoff was finally revealed in December 2008 and would be sentenced to 150 years imprisonment for running the world's largest ever Ponzi scheme defrauding investors of more than US\$10-17bio. Others not so large but still in the multi billion dollar range would follow, including Alan Stanford.

In 2010 Raj Rajaratnam a hedge fund billionaire would be arrested and he would receive 11 years imprisonment for insider dealing in the USA. In the USA and elsewhere prosecutions for both insider dealing, front running and market manipulation have dramatically increased.

Money Laundering

Insider Dealing

The detection, investigation and criminal prosecution of illegal insider trading and front or parallel running has become increasingly difficult. This is so for a number of reasons. Among other things, the sheer volume and complexity of modern stock trading heightens the difficulty of pinpointing specific illicit trades that were based on illegally acquired inside information. When an institution or a trader can move in and out of positions quickly and in large volumes, illicit trades become easier to mask, harder to find, and subject to plausible deniability. Moreover, in the modern information age, there has been a veritable explosion of newsletters, websites, blogs, tweets and feeds publishing every last rumour and report of potential mergers and acquisitions and earnings reports. That, of course, makes it easier for an accused insider trader to argue - in the absence of incriminating recorded evidence to the contrary - that any trades were based on some report somewhere, which may never have in fact been believed or even read.

Whilst many cases involve one or more family members co-investing based on inside information, more sinister insider rings have also been uncovered, of particular interest is the involvement of employees of financial institutions and hedge funds in these insider rings, expert networks and the techniques used by regulators and enforcement to uncover and prosecute them but also the lengths individuals go to hide their tracks.

Of course the most celebrated insider case remains the case of Ivan Boesky in the US who used offshore accounts to try to mask his involvement and who was convicted in 1987, and whose story inspired the movie "Wall Street". Boesky was at the centre and was the principal beneficiary of inside information from Wall Street insiders, who also benefited handsomely, alongside Denis Levene from Drexel Burnham Lambert, which had grown strong through its star banker Michael Milken. Soon after Boesky's fall and as a result of this investigation and prosecution links to Ernest Saunders and the Guinness 4 were uncovered and this scandal broke in the UK.

Prior to this and turning back the pages of history come the cases of Albert Wiggin and William Duer and since then there have been many cases where insiders, tipsters and tippees have all fallen foul of the law, some that simply couldn't resist, making money for a time for themselves friends and or relatives and others where the insider dealing is more premeditated, structured and organised and on more an industrial scale.

R Foster Winans who penned a weekly newspaper column called the "Herd on the Street" who traded ahead of his own tips prior to publication, Michael Guttenberg; Winifred Jiau; Ken Lay and Jeffrey Skilling of Enron, who as late as April 2001, before the company's collapse, the very same year alongside 27 other senior Enron executives sold overvalued stock for more than a US\$1bio not long before the company was declared bankrupt; Mehmit Sepil; and Nicos Stephanou; and most recently Raj Rajaratnam and others. Raj Rajaratnam, a hedge fund manager and founder of the Galleon Group, a New York-based hedge fund management firm who created an intricate system of paid insiders across the financial industry that he used to access information to benefit his hedge fund and himself as a result was prosecuted and convicted by US law enforcement who successfully employed tools that typically are used to combat organised crime (wiretaps, cooperators) catching, the ring being uncovered through links to the earlier case of Eric Franklin and others in 2006 where Linda Thomsen, the SEC's then enforcement chief, described the Franklin's insider trading activities as "one of the most pervasive Wall Street insider trading cases since the days of Ivan Boesky and Dennis Levine.

The Franklin case also involved Michael Guttenberg, an institutional client manager in UBS' equity research department in New York was arrested and sentenced in 2006 to six and a half-years in prison and ordered to pay back \$15.8 million he made from his involvement in an insider trading scheme involving several hedge funds. Guttenberg had access to potentially price sensitive confidential information due to his membership on the UBS's Equities investment review committee since 2001. As a member of this Committee, Guttenberg regularly had access to stock recommendations by influential UBS analysts before the information was made public. Guttenberg provided this information to two Wall Street traders, for example a 2006 downgrade of Caterpillar Inc., the world's largest maker of bulldozers, and a 2006 upgrade of Goldman Sachs Group to Erik Franklin and David Tavy, in exchange for a cut in the profits they made from trading on that information. Erik Franklin and David Tavy in turn cut more deals and gave tips to others who made money on this information. He also passed hundreds of tips to Tavy and Franklin. At a meeting at the Oyster Bar in New York's Grand Central Station in 2001, Guttenberg offered to settle a US\$25,000 debt to his friend Franklin, by slipping him analyst ratings in advance. At the time, Franklin was working at Bear Stearns in New York and managing money for Lyford Cay Capital, which invested some of Bear Stearns senior officials. He and his colleague, David Tavy made more

than US\$4mio on inside trades in brokerage accounts they controlled. Three Bear Stearns brokers also traded on Guttenberg's tips. He continued to do this from 2001 to 2006 and was paid hundreds of thousands of dollars, while others who were involved in this insider trading made more than US\$17.5mio. Guttenberg made similar deals with others, including another hedge-fund manager where he routinely provided tips about ratings changes on stocks such as Amgen Corp., Whole Foods Market, and Union Pacific Corp. He tried to cover his tracks by using coded text messages made from disposable cell phones, no use of e-mails, or telephone calls, not trading in his personal account, no wire transfers or cheques accepting monies only in cash.

In a separate but connected scheme, Randi Collotta was working as a compliance officer for Morgan Stanley in New York. Collotta worked with her husband a New York Attorney to leak price sensitive information to her friend Marc Jurman, a broker in Florida, and others for example in 2004 and 2005 information about Johnson & Johnson's failed US\$24.2bio bid for Guidant Corp., UnitedHealth Group Inc.'s US\$8.2bio acquisition of PacifiCare Health Systems Inc. and ProLogis's US\$5.5bio purchase of Catellus Development Corp were leaked. Randi and Christopher Collotta was sentenced to four years' probation and three years' probation respectively. In addition to Marc Jurman, the information was sold to Wall Street hedge fund traders including Erik Franklin at Bear Stearns. As an active Hedge Fund trader, Franklin thought he could bury these trades in the mass of trading conducted on the exchange and via his 50 to 100 different trades per day.

It appears that the SEC was able to pick up irregular profitable trading patterns in the merger and acquisition of two publicly traded companies, Adobe Systems, and its acquisition of Macromedia in 2005, and ProLogis, and its acquisition of Catellus Development. Once the SEC saw the irregular trading, they then focussed on those trading ahead of publicly available information, then matched these professional investors with other public deals to identify whether similar patters could be identified.

Another case worthy of closer attention is that of Chris Littlewood, his wife, and family friend Helmy Omar Sa'aid who all pleaded guilty in 2008 to insider dealing on the London Stock Exchange and AIM listed shares. Littlewood, who earned £350,000 a year working for German investment bank Dresner Kleinwort Wasserstein with access to inside information. Littlewood passed information to his wife who then passed this on to family friend Helmy Omar Sa'aid. The FSA investigation began in August 2008 when

a standard review of trading patterns ahead of the announcement of a possible takeover of a company revealed that Mr Sa'aid regularly bought a small number of shares in the company in the weeks before the announcement. Further investigation of Mr Sa'aid's trading activities revealed that he had made similar trades before 22 other merger announcements. The FSA checked and learned that one Bank had advised on 15 of those 22 deals, and therefore this was most likely the source of the inside information. The breakthrough in the investigation which tied Mr Sa'aid to Mr Littlewood came when the FSA checked Mr Sa'aid's bank accounts and found that a Ms Siew Yoon Lew paid money from her bank account into the account of both men. Siew Yoon Lew was the maiden name of Mr Littlewood's wife. Ms Lew was the conduit by which the insider dealing was conducted. Her husband passed information to her which she then made available to Mr Sa'aid, and after the deal had been made payment was facilitated through her bank account. Littlewood was sentenced to three years and four months in custody, Sa'aid to two years and Mrs Littlewood to twelve months, suspended for two years. Littlewood, 37, spied on colleagues to pass on information so that he and his wife Angie, 39, and her friend Helmy Sa'aid, 34, could make almost £600,000, on investments of £2mio on LSE shares purchased between 2000-2008 in what the judge described as "the biggest prosecution for insider trading ever brought."

Another case, also from 2008 involved Nicos Stephanou who was arrested on insider dealing charges on 27 December 2008, when his Cancun-to-London flight stopped at Newark Liberty International Airport. Stephanou had joined UBS in 2002 after working in the corporate finance department of Coopers & Lybrand LLP and the mergers and acquisitions group at Credit Suisse. Whilst at Credit Suisse in London, Stephanou became friends with Ramesh Chakrapani who later moved to the Blackstone group. In 2006, Nicos Stephanou was a member of the team at UBS that advised ABS on its response to an approach by a consortium of buyers looking to acquire the company prior to ABS publicly announcing that this approach would lead to an agreed takeover. Also in 2006, ELK publicly announced that it had agreed to be acquired by The Carlyle Group. ELK hired UBS as its financial advisor. Nicos Stephanou also worked on this deal. In late 2006, NHI publicly announced that it had retained Blackstone as its financial adviser to consider strategic alternatives and had received a buyout offer from its CEO, but stated that the offer was inadequate. Ramesh Chakrapani as an employee of Blackstone had access to material non-public information concerning this announcement by virtue of his membership of

the team at Blackstone that advised NHI on strategic choices. Ramesh Chakrapani and Nicos Stephanou each provided inside information they were privy to, to family members and to Joseph Contorinis, a hedge fund trader and personal friend at Jefferies Group. Nicos Stephanou, Ramesh Chakrapani and Joseph Contorinis were charged with insider dealing offences. In total, seven individuals were found to be engaged in the insider trading ring which generated a combined total of over US\$11.6mio in illegal profits. Nicos Stephanou served 19 months in custody after his arrest but was then freed following his co-operation in acting as the star witness in the trial and conviction of Joseph Contorinis who received 6 years imprisonment. For more details and case examples see Part 2, Section 7 and Section 8, including the case of SAC Capital in 2013, a Hedge Fund Group, who agreed to pay a record US\$616mio (2 cases US\$602mio and US\$14mio) to settle civil charges on insider dealing from the US SEC and later another US\$1.2bio in 2013.

Misuse of Information

Information that is confidential or owned by one party should not be misused by another party for that other party's own personal benefit. Prime examples include front running and parallel running.

Front/Parallel Running

Front Running / Parallel Running is an investing strategy that anticipates the impact of upcoming trades on the price of a security. In front-running, a person will take a position in a security just before a trade that will likely cause the stock to move in a predictable way is executed.

The most common example of front-running is when an individual buys shares of a stock for himself or for his firm or firms position, just before a large institutional order for the stock which will cause a rapid increase in the stock's price is executed. This information can be obtained legally through, for example, market information about impending trades, or illegally by hearing of new firm research or firm portfolio decisions, for example, by breaches in firms' Chinese Walls.

For parallel running the same applies except that the trading is done at the same time and not in front. A fine for Merrill Lynch in 2010 for front running resulted in a fine of US\$20mio. Other examples include Philip Jabre and GLG Partners, John Kaweske, Ken Mahaffrey and Dipak Patel. For more details and case examples see Part 2, Section 7 below and Part 2, Section 8 below.

Kidnap, Illegal Restraint & Hostage Taking

"If you're out there feeding the bears, the bears are going to keep coming into the camp"

Erik Rye, an adviser for hostage affairs at the US State Department referring to the payment of ransom demands¹

Harms

Kidnapping may seem to be an isolated crime that only affects the family and immediate community surrounding the victim, but its effects are broader than one may think. Through the payment of ransom demands, kidnapping funds terrorist organisations, organised criminal groups and any other criminal enterprise that chooses to use kidnapping as a source of revenue. In developing countries, kidnappings can have an even greater impact, especially high profile kidnappings of foreign expats, by discouraging tourism and foreign direct investment and even creating conditions that could spur human capital flight to neighboring countries.

In certain cases, kidnappings can damage foreign relations between countries. Several countries have policies against payments of ransom arguing the payments encourage more kidnappings. Other countries secretly succumb to the ransom demands and make payments to the kidnappers thereby frustrating and damaging relations with allied countries with policies against these payments.

Statistics

According to the Independent, a UK newspaper, at the end of 2010, US\$1.5bio was estimated to have been paid out in ransom to kidnappers around the world. 2011 statistics show reported kidnapping cases in many countries, or even cities, to be rising over the prior year. Another UK newspaper, the Times, reported that in 2011, there were around 2,954 cases of kidnappings reported across the Pakistani city of Lahore. In 2010, up to 2,831 people were kidnapped. Still, the most effective way to retrieve kidnapped family members is to pay the ransom.²

According to red24, a firm of security analysts, using a variety of criteria, including official and unofficial statistics, anecdotal evidence, overall crime levels and the kidnap risk posed by issues such as political instability, terrorism and police corruption. The countries that pose the greatest risk of kidnap are Afghanistan; Somalia; Iraq; Nigeria; Palestine; Yemen; Venezuela; Mexico; Haiti; and Colombia.³

Highest Risk Countries for Kidnap for Ransom	
1	Afghanistan
2	Colombia
3	Haiti
4	Iraq
5	Mexico
6	Nigeria
7	Pakistan
8	Somalia
9	Venezuela
10	Yemen

Source: red24 2012

In Afghanistan: there are around 950 kidnappings for ransom per year.⁴

In Somalia the piracy and kidnap offshore threat is well established: 24 vessels were seized in 2011 with over 400 hostages taken and 265 still held captive in 2012.⁵

Total ransom money paid to Somali pirates (US\$mio)	
2006	5
2007	25
2008	70
2009	80
2010	180

Source: FATF organised Maritime Piracy and Related Kidnapping for Ransom - July 2011⁶

In Iraq no official figures are available for 2011, but red24's anecdotal evidence suggests the risks remain high. The country provides a complex kidnapping risk environment with criminal, terrorist and politically motivated parties all carrying out kidnappings.⁷

In Nigeria the country records well in excess of 1,000 kidnappings for ransom a year.⁸

In Pakistan, official statistics reveal over 15,000 kidnappings a year and the true number is likely to be higher due to under-reporting.⁹ However, only 10-20% of abductions are for ransom.¹⁰

In Yemen over 200 foreign nationals have been kidnapped over the past 20 years.¹⁰

In Venezuela official statistics revealed over 1,000 kidnappings for ransom in the first ten months of 2011, and the country has one of the highest per capita rates of abduction in the world.¹¹

In Mexico official statistics for 2011 are likely to reveal over 2,000 kidnappings for ransom. However, the actual number is far higher and the Mexican NGO, Consejo para la Ley y los Derechos Humanos (CLDH), reported that its statistics revealed some 17,889 kidnaps.¹²

In Haiti, incident numbers now in the low hundreds, which is a significant decline on 2006 when some 720 incidents were recorded. However, a significant threat persists and per capita abduction rates are second only to Venezuela.¹³

In Colombia, despite a significant reduction in incidents over the past ten years, incident numbers in recent years are still high with 258 kidnappings recorded by the authorities in 2011.¹⁴

According to figures by the US National Counter-Terrorism Center, there were 6,050 people who were kidnapped and held hostage by terrorists around the world.¹⁵

According to the US Treasury Department, the average kidnap for ransom payment to Al-Qaeda in the Islamic Maghreb was US\$4.5mio per hostage in 2010. In 2011, the average amount of ransom paid increased to US\$5.4mio per hostage.¹⁶

Up to US\$70mio is estimated to have been paid to secure the release of Western captives since 2010 - an average US\$2.5mio per victim.¹⁷

Definition / Description

Kidnapping is the taking away of a person from one place to another against their will by force, fraud or threat and holding them in false imprisonment. Illegal restraint is when a person is kept in captivity by means of any form of physical restraint without the provision of a legal justification. Hostage-taking is the taking of a person in order to force a state or an individual to meet certain conditions such as releasing prisoners or paying of ransom. The FATF defined kidnapping, illegal restraint and hostage-taking as a predicate offence for money laundering in their 40 Recommendations.

The UNODC defines Kidnapping as the unlawful detention of a person or persons against their will for the purpose of demanding for their liberation an illicit gain or any other economic gain or other material benefit; or in order to oblige someone to do or not to do something. Once a person is kidnapped, they become a hostage; Hostage Taking is defined as the act of a person who seizes or detains and threatens to kill, to injure, or to continue to detain another person in order to compel a third party, namely, a State, an international intergovernmental organisation, a natural or juridical person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage commits the offence of taking of hostage.

The International Convention against the Taking of Hostages was adopted by the General Assembly of the UN in 1979 and makes hostage taking an offence.

In 2003, the Trafficking in Persons Protocol aka Palermo Protocol (Protocol to the Convention against Transnational Organised Crime 2000) was enacted to prevent, suppress and punish trafficking in persons. Further to this, in 2004, the Smuggling of Migrants by Land, Sea and Air aka Palermo Protocol was adopted by the UN as supplement to the Convention against Transnational Organised Crime.

Historical Background / Context

Charley Ross a 4 year old boy earned the unfortunate distinction of being the first American to be kidnapped for Ransom in 1874. 2 days after the Kidnap a ransom note demanding US\$20,000 was sent to the family home. Unfortunately following leads the Police searched for and shot dead the suspected Kidnapper before he could be interrogated to locate Charley who was never found.

Whilst the Ross case caused a stir in Philadelphia the kidnapping of the Charles Lindbergh Jr at only 20 months old caused a sensation in 1932. A ransom of US\$50,000 was a paid but no baby was produced. The baby would be found dead 2 months later 7 kms from the family home. The Police eventually located part of the paid ransom and executed burglar and armed robber Bruno Hauptmann for the kidnap and death.

It would take until 1963 before another high profile kidnap case would make the media spotlight, when Frank Sinatra's son was kidnapped from a hotel room and a demand for US\$240,000 was later made. Sinatra with an FBI agent himself delivered the ransom and his son was soon released. The Kidnappers were later caught by the FBI. Sinatra sent US\$2,000 gold watches to the FBI agents involved and to FBI Chief J Edgar Hoover. The former returned them reminding Sinatra they were not allowed to accept gifts. Hoover didn't return his!

Ten years later in 1973 the grandson of perhaps the worlds richest man - John Paul Getty was kidnapped in Rome. The Getty family suspected their grandson may be playing a hoax and they refused to pay the ransom of US\$500,000 believing the sum claimed so small as to be likely to be a stunt. The demand went up to over US\$16mio but still the Gettys refused to pay. J Paul Getty said that "acceding to the demands of criminals and terrorists merely guarantees the continuing increase and spread of lawlessness."

It took the delivery of the cut off ear of the young man before the seriousness of the situation was fully appreciated but even then only US\$3.2mio was paid

and the grandson was returned. The money was handed over in 3 sackfulls of banknotes and was never recovered.

In Italy in 1978, a former Prime Minister and Presidential prospect Aldo Moro was on his way with 5 bodyguards to see the then Italian Prime Minister when his car was ambushed by the Red Brigades, an Italian Terrorist group. All 5 bodyguards were shot and Moro taken. The terrorists demanded the release of 14 Red Brigades members imprisoned in Italian Jails. The Italian government refused to negotiate on principle and Moro was found murdered. Eventually in 1983, 32 terrorists were convicted on various charges connected with the Kidnap and Murder.

In the 1970s up until the early 2000s, South America was the hotspot for kidnappings and Hostage Takings accounting for 65% of all kidnap cases worldwide (4). Groups like the Revolutionary Armed Forces of Colombia (or FARC) and the National Liberation Army (or ELN) thrived on Kidnapping as a source of revenue for their operations. The FARC's most famous kidnapping was of a Colombian politician and French dual national Ingrid Betancourt. Outside of South America, Kidnapping was commonly used to publicize the cause of an insurgency or for the exchange of political prisoners, military prisoners or the release of other opposition members/leaders. Although this type of exchange still exists, for example the Gilad Shalit incident where an Israeli soldier was abducted in 2006 by Hamas and was then released in 2011 in exchange for 1,027 Palestinian prisoners, most of the kidnappings today are of foreign nationals in exchange for an exorbitant monetary ransom demands.

Money Laundering

The shift to Kidnapping as a main source of revenue has gained popularity over the past four to six years and in most jurisdictions the number of Kidnapping is only increasing. The growth is being exacerbated by the emergence of insurance companies that sell kidnap and ransom insurance (or K&R insurance) and by countries that agree to pay ransom demands for their citizens who have been kidnapped and taken hostage. Certain countries have strict, public policies that forbid negotiating with a kidnapper's ransom demands. However the problem remains since most of the ransom demands are negotiated by private, well paid negotiators who are able to coordinate the release of a hostage and the successful payment of the ransom.

Terrorist Groups and other Organised Criminal Gangs have recognised Kidnapping as a viable source of revenue. For instance, the average ransom paid in 2008

to Somali pirates was estimated to be US\$1.25mio. The average ransom paid in 2010 to Somali pirates was US\$5.2mio with ransom payments in excess of US\$9.2mio.¹⁸ The Transitional Federal Government of Somalia is powerless to stop Piracy and hence the Kidnapping of pirated ships and their crew are still taking place off the Somali coast.

Kidnapping have been most rampant in environments similar to Somalis as a FATF report on Kidnapping for Ransom mentioned that most Kidnapping today take place in politically unstable countries where central authority is often weak, public and private corruption is endemic and the social fabric of those nations has unraveled to a considerable degree.¹⁹

Some of the current hot-spots for K&R by Terrorist Organisations are in African Sahel, the Philippines, Pakistan and Afghanistan. In 2012, the average ransom demand by kidnappers in Nigeria was US\$490,000, with the average amount actually paid approx US\$50,000. Recently, the Interior Ministry of Pakistan reported that there were 474 cases of Kidnapping for Ransom in 2010, and 467 Kidnapping for Ransom cases in 2011 with the average ransom demand between US\$500,000 to US\$2.2mio.²⁰ And between 1992 and 2010, militant organisation Abu Sayyaf in the Philippines earned an estimated US\$33mio from Kidnapping foreigners and holding them for ransom.²¹

In the wake of the 11 September attacks on the World Trade Centre and the Pentagon, a report was issued that tried to identify the main source of revenue for Al-Qaeda and other Terrorist Organisations. It was reported that Terrorist Organisations used the drug trade, of mainly opium and cocaine, as one of the main sources of revenue. Fast forward to 2012 and one of the main sources of revenue for Terrorist Organisations is Kidnapping for Ransom.

As reported in Newsweek, since the beginning of the Iraq war according to US government figures, hundreds of foreigners from more than 10 different countries were taken hostage in Iraq. These numbers are small in comparison to the kidnappings of Iraqis, which took place at the rate of 10-30 per day, at one time mainly for purposes of ransom. However, it is not just the Terrorist Organisations that are profiting from Kidnapping. Other groups have started to use Kidnapping to fund their operations, like the Somali Pirates in the waters off the Horn of Africa, Mexican Drug Cartels and Organised Crime syndicates around the world.

According to EU and US government experts Al-Qaeda in the Arabian Peninsula (AQAP) and the Organisation

of Al-Qaeda in the Islamic Maghreb (AQIM) see K&R as a primary source of revenue. The profits gained from K&R by groups such as AQAP and AQIM are usually sent outside the region to other affiliates of Al-Qaeda to help fund their terrorist activities/operations. In 2010, captured financial documents from Al-Qaeda in Iraq (AQI) showed expenditure data with 56% of the profits from K&R going to the funding of AQI operations in other regions.

At the end of 2010, an estimated US\$1.5bio was estimated to have been paid out in ransom to kidnappers around the world,²² posing a real threat to the global financial system. Of that total, US\$180mio was paid to Somali pirates where 80% of the ransoms are in the form of physical cash and delivered in bulk cash by air drop off the coast of Somalia with the average payout at almost US\$5mio. These bulk cash payments pose large problems for law enforcement who attempt to track the money. For one, the ransom payments often do not result in bulk cash disclosures/declarations and/or suspicious transactions reports to the Financial Intelligence Units. Additionally, once the cash is in the hands of the pirates and the ransom payment is divided to the individuals who helped coordinate the attack, the profits are occasionally put into real estate purchases in northern Somalia or in neighboring Kenya. The FATF report on Maritime Piracy says there is debate about whether pirates based in Somalia use Hawalas, with some experts suggesting that most hawaldars cannot handle the amount of cash that ransom payments bring in.²³ However, some law enforcement believes that ransom payments could be moved through Money Services Businesses (including informal MSBs such as Hawalas). For more details on MSBs including Hawalas see Part 1, Section 2, Sub-section 2.

The FATF report on Kidnapping for Ransom analyzed K&R cases involving Terrorist Organisations and one fact was prominent throughout. The formal financial system and banks in particular, played a surprisingly significant role. The reason for the bank's role is the victim's family or the victim's representative are located in developed areas with sophisticated banking systems, which gives them the ability to pay a large ransom demand. Therefore, the FATF report believes that banks may be at risk for placement and transmission of ransom payments. Excluding the Somali pirates, cash still played a significant role in these K&R cases. Unfortunately, when terrorist demand the ransom payment be made in cash the money trail grows cold after a short time and to further complicate the matter the Kidnapping can occur in one jurisdiction but the ransom may be paid in another.

At the recent G8 Summit hosted by the UK in June 2013, the hosts included a proposal to stamp out ransom payments as many are considered to fund terrorist groups. Up to US\$70mio is estimated to have been paid to free western hostages in the last 3 years, at an average of US\$2.5mio for each captive. Whilst the UK already outlaws such payments, other countries such as France, Italy and Japan are suspected of still allowing such payments though agreed at the G8 Meeting as a G8 announcement to ban such payments going forward.

The fact that some G8 Western citizens are targeted is thought to have a lot to do with both the price that can be obtained and the reaction that a kidnaping receives. Whilst an agreement to refuse to pay ransom demands is one approach another not adopted could have been suggested by at least one of the G8 members.

A leading western hostage negotiator has for example claimed that some countries have taken a much more aggressive approach, recounting a claim about a Hezbollah kidnaping of a Russian. In response the Russian security service's response was to allegedly find one of the kidnap-gang relatives, cut off his private parts and send it to the kidnappers. "Unsurprisingly they got the hostage back." said the negotiator.²⁴

In response to the threat of kidnap, the demand for kidnap and ransom insurance (K&R) in recent times has been good. Many of the worlds biggest companies now have some K&R coverage for their staff. Plans typically cover the costs of ransoms, the hiring of consultants and negotiators, lost earnings and other costs. The insurance policy doesn't pay the ransom, but pays out to the Insured if a ransom is paid by the company or on its behalf. The market in 2006 was estimated to be worth approx US\$250mio in 2006 which has since doubled in size by 2011. Still insurers report the market is shifting. Somali piracy has dropped off; there have been no documented successful hijackings since May 2012. And although the number of attacks in the Gulf of Guinea overtook those of the East Africa in 2012, quieter shipping lanes there mean fewer potential customers. Yet new markets are opening up. In Africa, India and Latin America the middle class has been growing—and so has the worry about being kidnapped. For instance, "express" kidnapings are on the rise, negotiators report. Unlike the protracted kidnap the new version entails fast, targeted grabs, followed by shorter periods of detention and smaller ransoms.

Market Manipulation

"the traders had been "knuckleheaded"

Former Citi Chairman and CEO Chuck Prince, 2004, following the revelations surrounding the so called "Dr Evil" trades which resulted in a large fine and censure¹

Introduction

The trading volumes in global markets, equities, securities, commodities foreign exchange and derivatives markets have grown dramatically throughout the 20th Century, providing ever more opportunities for those that seek to profit from illegal fraudulent activities.

In many parts of the World, initially in the West, but now beyond, Markets have been relied upon to drive economic growth. There are many hundreds, if not thousands of examples though, through the years of significant abuses perpetrated on market participants, including investors, that have unfairly disadvantaged the abused and undermined the integrity of the markets involved, including manipulating behaviour. A number of these events, which proved most damaging, led to increased governmental intervention to regulate so called free markets.

For those involved regularly in the Markets including professional market participants, they must rely on the legitimacy and integrity of these Markets for their own trades and for those of their customers. Professional Market Participants therefore have a special responsibility to ensure the continued legitimacy and integrity of these Markets, to ensure their own actions, nor those of their clients amount to a manipulation, rather they should contribute to Market integrity by having strong, clear policies and effective controls to protect both own reputation and that of the Markets themselves.

Harms

Market Manipulation is both a theft and a financial Fraud. The victims are all those market participants that play by the rules, investing honestly. The abuser when he manipulates cheats every other participant and offends the principles of the Markets that honest participants rely upon.

Markets need to be organised in a way that encourages all investors to trust that they will be treated fairly. Any appearance that the markets allow some to trade using an unfair advantage against investors at large will harm that trust and discourage participation in those markets.

The public cost, which is the harm done to the integrity of the market and to confidence (i.e. perceptions of the integrity of the market), can lead to changes in broader market behaviour and pricing, and flow on into other adverse effects on the economy.

Conceptually, the public cost of market abuse including manipulation can be expected to be seen in the first instance in a widening in the bid - ask spreads for all trading in the securities in question. This can spill over into widening bid - ask spreads in the market for all securities, an increase in the cost of capital and a reduction in the market price of securities - not only for new and existing issues of the security in question but also for other securities. A reduction in market depth (reflecting reduced willingness to trade) and reduced trading volumes could also be expected.

These higher costs of capital and costs of trading could feed into lower returns on investment, less fixed capital spending and less potential and actual economic demand and activity over the economic cycle.

Unless they are caught and punished adequately, market abusers and manipulators themselves do not incur much of these economy-wide costs. The conduct also creates a negative externality. Securities prices in the market are distorted and consequently other buyers and sellers end up paying for inefficiencies in the market as a result of the offender's conduct.

Statistics

Whilst there are few statistics available to demonstrate the size and scope of manipulative activity and their consequences, recent fines announced with more likely to follow with respect to the Libor Scandal demonstrate the potential harm that can result, particularly where collusive practices appear to be at work.

Outside of the Libor Scandal, there were also suspicions that manipulative actions may also have played a role in creating the financial crises of 2007.

Whilst it is widely accepted that the underlying causes of the crises were the weaknesses in the US Housing and mortgage sector, the existence of "Bear Raids" just prior to the autumn of 2007 suggests that it too may have contributed to the crises.

The crises to date has resulted in widespread economic damage and questions over the very nature itself of market themselves. The US Financial Crises Inquiry Commission (FCIC)² reported³ that over 26 million Americans were unemployed or underemployed by early 2011 and that nearly US\$11 trillion in household

wealth had evaporated. The FCIC also concluded that the crises though was avoidable and was caused in part by “widespread failures in financial regulation and supervision that proved devastating to the stability of the nations financial markets.”

Annual enforcement statistics provided by the SEC from 2003 to 2012 show a total number of enforcement cases across all manner of violations, including insider dealing, Market Manipulation and others, rising in 2003 from 679 to 734 in 2012. Insider dealing and Market Manipulation made up; 50/32 and 58/46 cases respectively.

Definition/Description

According to the UK's FSA as set out in their Code of Market Conduct³ (August 2009),³ Market Manipulation is included within the definition of Market Abuse that includes (i) insider dealing and improper disclosure, (ii) misuse of information, and (iii) market manipulation including: (a) manipulating transactions, (b) manipulating and “fictitious” devices, (c) dissemination of information, and (d) misleading behaviour and distortion. This effectively applies EU law as set out in the Market Abuse Directive, which is expected to be updated and reissued as MAD 2. For more details see Part 1, Section 3, Money Laundering Laws & Regulations. As for Insider Dealing the US relies on broad anti-fraud provisions contained in the federal securities laws, e.g., Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5. For more information see Insider Dealing above. FATF have included market manipulation alongside insider dealing as a predicate offence for money laundering in their 40 Recommendations.

Historical Background / Context

For a comprehensive history of market abuse as it applies to both Insider Dealing and Market Manipulation see Inside Information above which is not duplicated here.

Money Laundering

Market manipulation is the practice of interfering in the market by manipulating transactions, using manipulating and “fictitious” devices, disseminating false or misleading information or by undertaking distorting or misleading behavior. Manipulators and abusers have included regulated financial institutions, but more often rogue employees, as well as lightly or unregulated ones, including Hedge Funds and in particular of concern are Boiler Rooms. For more details see Part 1, Section 1, Fraud, incl Tax Fraud and Cybercrime.

Top Major Market Manipulation Techniques	
1	Abusive Rate Fixings / Intimidation / Co-ordination
2	Abusive Short Selling
3	Abusive Squeezes / Cornering / Warehousing
4	Banging / Marking the Close / Marking the Open / Portfolio Pumping
5	Bear Raids / Short & Distort / Trash & Cash
6	Front Running / Parallel Trading / Piggy Backing / Tailgating
7	Late Trading / Market Timing
8	Layering / Spoofing
9	Painting the Tape
10	Ping Orders
11	Pump and Dump / Hack Pump & Dump / Ramping / Scalping
12	Quote Stuffing
13	Rumoring / Puffing
14	Wash Trades / Circular Trading / Pre-arranged Trading / Soft Dollar Arrangements
15	Large and Unusual orders, including unusual order price, size etc

Source: Author

Both Boiler room operators and other rogues will use common schemes and techniques to make money unfairly and illegally in the securities markets, as did Stratton Oakmont using Pump and Dump schemes involving Penny Stocks. The following are brief summaries of these and many more abusive and manipulative practices, schemes and techniques.

Abusive Rate Fixings (Intimidation/Co-ordination)
The submission of rates at unrepresentative levels with the aim of distorting the respective benchmark which they are used to calculate. Following the revelations around the Libor and other benchmark interest rate fixings, by a number of rate setting Investment Banks that colluded to manipulate rates to benefit their own trading positions, rule changes are expected to ensure that manipulation around the setting of these rates are expressly covered by Market Abuse legislation / regulation going forward. Despite a lack of express regulation covering rate setting, a number of individuals involved are facing criminal prosecutions. The Libor benchmark interest rates are used to set an estimated US\$800 trillion-worth of financial instruments. For more details see Libor Bid Rigging Scandal in Part 2, Section 8, Enforcement Cases below.

Abusive Short Selling (See Short and Distort, Trash and Cash).

Abusive Short Selling involves short selling a stock while smearing the company with rumours to drive the stock price down, essentially the opposite of pump and dump.

Abusive Squeezes (see Cornering)

The ability to manipulate the supply or demand for an investment through the holding of a significant position. Where the owner of the security tries to distort the price at which others have to deliver, take delivery or defer delivery to satisfy their obligations.

Amends

High numbers of trade amendments, often with a large P&L impact are used by rogue traders as a way of masking their fictitious or fraudulent trading activity.

Backing Away

A backing-away occurs when a market maker firm fails to honour its obligations in a given security to honor the quoted bid and ask prices for a minimum quantity. This requires a market maker to execute an order “presented” to it at a price at least as favorable as its published quotation up to its published quotation size. A market maker’s obligation to fill an order begins generally at the time the order is “presented,” regardless of how the order is transmitted to the market maker.

Banging the Close

Where a trader, for example, buys or sells a large number of futures contracts during the closing period of a futures contract in order to benefit an even larger position in an option, swap, or other derivative that is cash settled based on the futures settlement price on that day.

Bear Raids (see Short and Distort and Trash and Cash)

Bear raids can be an illegal market practice where investors take a short position in a stock, disseminate negative news and then collectively sell borrowed stock. They profit by buying shares to cover their borrowed positions at a lower price.

Best Execution (See Excessive Mark Ups)

Brokers must obtain best execution for customers and must not charge customers excessive fees.

Bucketing

Where a broker executes a customer’s order for his own account instead of on the market, with the hope of profiting from a beneficial transaction at a future time.

Bucket Shop

Originating in the late 19th century, bucket shops

were a trading venue for the man on the street set up in rudimentary premises such as a café or hotel, akin to a betting shop, where an internal market was made for bets to be placed on stock prices. These days the term can be used to describe small, independent online spread-betting companies.

Cancellations

See Amends, trade cancellations are often used alongside trade amendments for the same purpose.

Capping

Effecting transactions in an instrument underlying an option shortly before the option’s expiration date to depress or prevent a rise in the price of the instrument.

Cherry Picking

Where a broker or investment manager takes all the beneficial trades for himself, rather than offering those trades to customers.

Churning

The excessive buying and selling of securities in a customer’s account by a broker for the purpose of generating commissions.

Circular Trading (see Wash Trades)

A fraudulent trading scheme where sell orders are entered by a broker who knows that offsetting buy orders, the same number of shares at the same time and at the same price, either have been or will be entered.

Cornering (see Abusive Squeezes)

Securing such relative control of a commodity that its price can be manipulated, that is, can be controlled by the creator of the corner.

Crossing Trades (see Wash Trades)

These are transactions where both buy and sell orders are entered at, or nearly at, the same time, with the same price and quantity by the same party, or different but colluding parties.

Curb Trading

Trading by telephone or by other means that takes place after the official market has closed and that originally took place in the street on the curb outside the market.

Directed Trading (see Soft Dollar Arrangements)

This is the practice of a fund adviser sending trades to a specific broker-dealer for execution (“directing” the trade), often in exchange for some benefit to the advisor, such as additional shelf space for its products. The broker-dealer gains because it receives the commissions from placing the trades (the “brokerage”). This practice

can create a conflict of interest between the investment advisor and the investor because the advisor may be tempted to direct trades to the broker-dealer that sells the most of the advisor's fund's shares, rather than the broker-dealer that provides the best execution or best price for trading.

Fictitious Orders (see Phantom Orders)

A trade that is designed to look as though a trade has been entered but has not been executed in fact.

Front Running

When a broker trades on the basis of non-public information about an impending trade. For example, if a broker knows a client is selling a large amount of stock in a particular company, enough such that the price of the stock will likely fall, the broker could sell or short that stock before executing the client's sale.

Ginzy Trading

A trader, in executing an order, particularly a large order, fills a portion of the order at one price and the remainder of the order at another price to avoid exchange's rules against trading at fractional increments or "split ticks."

Hack, Pump & Dump (see Pump & Dump)

In this form a person purchases penny stocks in advance and then uses compromised brokerage accounts to purchase large quantities of that stock. The net result is a price increase, which is often pushed further by day traders seeing a quick advance in a stock. The holder of the stock then sells his stock at a premium.

Insider Dealing/ Trading

The buying or selling of a security by someone who has access to material, non public information about the security.

Inter-positioning

Interposing another party between a trader itself and the market in a manner inconsistent with best execution requirements in particular inter-positioning can result in fraud where it results in the charging of excessive and undisclosed markups".

Intimidation/Coordination (Abusive Rate Fixings)

Coordinating its prices (including quotations), trades, or trade reports with other traders; directing or request another trader to alter a price (including a quotation); or engaging, directly or indirectly, in any conduct that threatens, harasses, coerces, intimidates, or otherwise attempts improperly to influence another member. This includes any attempt to influence another member to adjust or maintain a price or quotation and refusals

to trade or other conduct that retaliates against or discourages the competitive activities of another market maker or market participant.

Laddering

This refers to the practice where, a broker for example, in the context of an IPO, requires IPO investors to buy shares at higher prices in the after-market as a condition for receiving lower priced shares in earlier allotments.

Large and Unusual Orders

Trades of significance that are large and/or unusual when viewed against the ordinary course of business and/or versus the market.

Late trading

Late trading is the practice of placing orders in securities, for example, mutual fund shares after regular market hours, for example (a mutual fund will calculate its net asset value typically at 4:00 p.m. In New York for US funds), and so this practice can enable traders to capitalize on market-moving information which is released after the close of regular trading.

Layering (see Spoofing)

Multiple orders are submitted at different prices on one side of the order book slightly away from the market prices. This gives a false impression of the demand prompting a move in the share price.

Excessive Mark-ups

Excessive mark ups, or charging a customer a price significantly over the fair market price, for example whilst a trader is entitled to make a profit mark ups of 35% over the market price are very likely excessive. Undisclosed mark-ups in excess of 10% are potentially excessive too.

Marking the Close

Attempting to influence, for example, the closing price of a stock by executing purchase or sale orders at or near the close of the market..

Marking the Open

Attempting to influence, for example, the closing price of a stock by executing purchase or sale orders at or near the open of the market.

Matched Order

Matched orders are orders to buy or sell a security while entering (or knowing another person is entering) an opposite order for the same security at the same time and price, with the aim to give an impression of increased volume.

Momentum Ignition

Initiating or enhancing a trend through the aggressive placement of orders in the hope that others will follow, which creates an opportunity to reverse a position.

Naked Short Selling

Where a trader sells short a security without owning, or having arranged to borrow, the security. Firms normally locate securities available for borrowing prior to effecting a short sale in any security for its own account or the account of any customer, even if the short position is to be closed out by purchasing securities the same day.

Painting the Tape

An illegal action by a group of manipulators buying and/or selling a security among themselves to create artificial trading activity. The reference to the tape is a reference to the tape which was a running public display of market prices.

Parking

When parking shares, firms are attempting to cover undeclared short positions left over from transactions whose stock was not delivered by the settlement date. Rather than performing a buy in transaction, these firms collude with one another and by delaying the settlement process, inflate the number of shares available for trade in the secondary market.

Penny Stocks

Whilst Penny Stocks are a legitimate security to want to own, they are also vulnerable and often used in a number of common Manipulation schemes; including, **Cornering; Pump and Dump**, including the **Hack Pump & Dump**, followed by the **Short & Distort** otherwise known as the **Trash and Cash**. Such schemes use low priced securities ("Penny Stocks") that do not trade on major exchange, but rather Over The Counter (OTC) or on Bulletin Boards (In US as Pink Sheets). These stocks are more susceptible because: i) they typically have a low trading volume, ii) in some jurisdictions, there is no regulator or they are exempt from filings, iii) large amount of shares (control of float) can be obtained cheaply or fraudulently, and iv) trading can increasingly be done through internet-based accounts and private shell companies. The same principle applies in the UK, where target companies are typically small companies on the AIM or OFEX. In 2009, FATF in its report, Money Laundering and Terrorist Financing in the Securities Sector,⁴ identified Penny Stocks as a specific concern for Money Laundering/Terrorist Financing vulnerabilities because they are often used by criminal organisations to generate illicit assets through market manipulation, insider

trading, and fraud; and can be acquired by investing illicit assets into a company that is about to become public as a way of laundering funds.

Phantom Orders

A trade that is booked with an execution date far in the future, and is adjusted to include the correct settlement and trade date when the transaction is completed.

Piggy Backing

When a broker or adviser buys or sells a security for a client and then immediately makes the same transaction in his or her own account.

Ping Orders

The entering of small orders in order to ascertain the level of hidden orders and is particularly used to assess what is resting on a dark platform or within dark pools.

Ponzi Scheme (see Fraud above)

Ponzi scheme is an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors. Ponzi scheme organisers often solicit new investors by promising to invest funds in opportunities claimed to generate high returns with little or no risk.

Portfolio Pumping (see Marking the Close)

The illegal act of bidding up the value of a fund's holdings right before the end of a quarter, when the fund's performance is measured. This is done by placing a large number of orders on existing holdings, which drives up the value of the fund.

Pre-arranged Trading

Trades where an offer to sell is coupled with an offer to buy back, or where an offer to buy back is coupled with an offer to sell, at the same price or some other pre-arranged price that benefits the dealers or brokers engaging in the pre-arranged trading.

Puffing (see Rumouring)

Subjective, usually extraordinary, claims as to the merits of something, including a security, with little or no basis

Pump and Dump (see Hack Pump and Dump)

A scheme that attempts to boost the price of a stock through recommendations based on false, misleading or greatly exaggerated statements. The perpetrators of this scheme, who already have a position in the company's stock, sell their positions at the higher share price. Pump and Dump schemes usually target micro and small cap stocks (see Penny Stocks above), as due to the small float of these types of stocks it does not take a lot of new buyers to push a stock higher.

Quid Pro Quo Arrangements

For example Laddering or purchases or participation in future offerings by a client (so-called “tie-in” agreements), or the receipt of excessive compensation for other services provided.

Quote Stuffing

The submission of a large volume of orders to the market with the intention of slowing down the trading systems of other traders or market participants or hiding one's own strategy.

Ramping

The practice of trying to boost the price of a share and the company behind it by buying the securities in the market with the object of raising demand. If the price rises, the ramper may be able to make a quick profit by selling

Rumouring (see Puffing)

Disseminating false or misleading information about companies. Rumours have generally been considered unsubstantiated unless verified by an appropriate official of the company they concern.

Scalping

Scalping is when a broker, analyst, or other securities professional recommends that an investor buy a security and then sells that security at a profit immediately after the recommendation has been disseminated and investors have driven the price of the security up with their purchases.

Selective Issuer Disclosure

Where issuers of securities selectively disclose material, non-public information to analysts, institutional investors, and others, without also disclosing it to the public generally. Where disclosure is made intentionally, the issuer must “simultaneously” disclose such information to the public and where information is disclosed unintentionally, such information must “promptly” be disclosed to the public.

Short and Distort (see Abusive Short Selling and Trash and Cash)

When traders manipulate stock prices in a bear market by taking short positions and then using a smear campaign to drive down the target stocks.

Snake Trading

Searching order books in an attempt to find market orders for securities in which no bid or ask prices exist and then subsequently entering bid or ask prices that significantly vary from the normal market price of those securities.

Soft Dollar Arrangements (see Directed Trading)

Arrangements where investment advisers are given certain benefits (such as research) from a broker-dealer in exchange for the adviser directing trades to that broker-dealer for the broker-dealer to execute for a fee. These arrangements may generate a conflict of interest in some cases between the adviser's clients' interest in cheap and efficient brokerage services and the adviser's desire to use a broker that provides the most benefits to the adviser.

Spinning

Where investment advisers allow preferred customers to purchase shares in initial public offerings of stock (IPOs).

Spoofing

The entering of orders to create the impression of liquidity in a stock when the trader's actual intention is ultimately to trade in the opposite direction. The initial orders are then quickly cancelled or withdrawn, with the trader then making real trades if prices have moved to the trader's advantage.

Trade Shredding

Splitting any order into multiple smaller orders for execution, or any execution into multiple smaller executions for transaction reporting for the primary purpose of maximizing a monetary or in-kind payment or the transaction reporting of such executions.

Trash and Cash (see Abusive Short Selling and Short and Distort)

Involving the circulation of damaging information about a share that has recently been sold, with the intention of repurchasing it at a lower price.

Tailgating

Similar to front running, this is a practice that involves a broker buying or selling a security for his / her client and then immediately placing the same trade on his / her own account.

Tipping

Providing material non public information to another individual in breach of a fiduciary duty or other similar duty of trust, for the purpose of allowing the “tippee” to profit from the tip.

Unauthorised Trades

Broker-dealers entering into orders without the expressed and detailed permission of the customer unless the firm has been granted written discretionary authority by the customer.

Unsuitable Trades

A broker-dealer must have reasonable grounds for believing each recommendation to a customer is suitable on the basis of the customer's other securities holdings and financial situation, among other factors.

Unusual Order Price

Placing a sizeable order in a security at a price that is materially higher or lower than the bid / ask in order to inflate or deflate the market price of that security.

Warehousing

Holding a sizeable portion of a security / commodity in order to create an artificial shortage in the market which can benefit the holder when the excess demand causes a spike in the price.

Wash Trades (see Circular Trading)

Trades involving no change in beneficial ownership; i.e. buying and selling the same number of shares at the same time at the same price—often to artificially increase the reported volume of trading in that security (in practise there may be small variances across both size and price). It should be noted that in a number of cases investigated during the [Libor Scandal](#) wash trades were used to facilitate unauthorised payments to brokers as rewards for their efforts to manipulate Libor.

Vulnerable Markets and Notable Cases

Many of these schemes have been employed on the equities markets, focussing on a particular stock, so that individual actions can have an effect, for example three of the most notorious of America's so called [Robber Barons](#); [Daniel Drew](#), [Jay Gould](#) and [Jim Fisk](#) were serial manipulators at a time before rules were established as were [Michael Meehan](#); [Charles Mitchell](#); [Richard Witney](#); all who would become infamous due to their activities before during and after the [Stock Market Crash of 1929](#).

Despite regulation, there have been plenty of examples of manipulators who seek to make money for themselves unfairly at the expense of others, using techniques of old and applying them to new models, markets and investors.

It is also possible to manipulate and use many of the schemes seen above beyond individual equities, to securities and to particularly securities markets and their derivatives even though the larger the market the harder it is to manipulate.

There are also, beyond the securities markets cases where serious manipulation has been attempted for example in the Commodities and Precious Metals markets, for

example by [Yasuo Hamanaka](#) who attempted to corner the copper market in the 1990s and before him the [Hunt Brothers](#) who tried a decade or more earlier to do the same in silver. These markets work in similar ways to the securities markets and are regulated in a similar way. For example, market participants may attempt to illegally manipulate the market for a commodity by such actions as fraudulently reporting price information or cornering the market to artificially increase the price of the targeted commodity. This is of particular concern when it affects delivery of the underlying commodity which may be needed by commercial enterprises for their business activities. For notable examples see the cases of [Lui Qibing](#); [Yasuo Hamanaka](#); the [Hunt Brothers](#); and [Christopher Pia](#).

Whilst some markets appear too big to manipulate, for example the foreign exchange markets, sometimes to the disappointment of Central Banks who are legally entitled and do still try, in order to try to manage their exchange rates, the conventional wisdom that some markets are therefore free of manipulation or rules and regulations, monitoring and surveillance is not required needs a reality check particularly as we see from the [Libor Bid Rigging Scandal](#). For details see Part 2, Section 8, Enforcement Cases below.

Major cases include those best known from history including way back to the [Tulip Bubble](#) bursting in 1634, followed by the bursting of the [South Sea Company](#), [William Duer](#), [London Stock Exchange](#) hoaxes of 1814, NY State Senator [Kimble](#) in the 1840s, the [Robber Barons](#) including [Daniel Drew](#) and [Others](#) and the [Stock Market Crash of 1929](#). More recently also in the 1970s with the [Hunt Brothers](#), Michael Milken in the 1980s followed by [John Kaweske](#), the [Flaming Ferraris](#), the [California Electricity Crisis](#), [Shell](#), [Ken Mahaffey & Others](#), [Simon Eagle](#), [Christopher McQuoid](#), [Dipak Patel & Others](#), [David Mason](#) and [Christopher Pia](#). For more details see Part 2, Section 7, Criminal Cases, Market Abusers below. Most recently the action against [Panther Energy Trading](#) for market manipulation was announced in connection with High Frequency Trading. For more details see Part 2 Section 8 Enforcement Cases below.

Murder & Grievous Bodily Injury

"Murder is unique in that it abolishes the party it injures, so that society has to take the place of the victim and on his behalf demand atonement or grant forgiveness; it is the one crime in which society has a direct interest"

W. H. Auden, English Poet

Murder is perhaps the single most serious criminal offense and is one of the oldest crimes since the beginning of organised society. Every major religious text forbids the act of murder with the exception of warfare, capital punishment, self defence, etc. The threat of violence to a person or their loved ones is a persuasive technique used by Organised Criminal Gangs to run and fund their criminal enterprises and to keep those involved silent on the details. Intimidating and scaring people with the risk of torture and ultimately the loss of their lives is an act of terrorism that is used by Terrorist Groups in the hopes of bringing about religious, political or other changes to society.

Harms

When a person is murdered, the affects are felt immediately by the surrounding community. However, when the victim is a Political Leader, the affects can be felt by an entire society. The murder of a senior public official, is usually described as an assassination (murder with a political motivation).

Since murder can have a profound affect on society, the act of murder on community leaders or public officials is commonly used as a tool to sway public opinion. When an assassination is carried out, it is usually not planned by a solitary individual but rather it is conspired by a group of individuals with a political, religious, ideological or military motive, including Organised Criminal Gangs and Terrorist Groups know and understand the affects on society of murder and use it to further their own criminal or terrorist agendas.

Another particular group of professionals that are threatened with murder or bodily harm are journalists. The International Federation of Journalists reported in 2010 that almost 100 journalists were murdered because of their work.¹ Professionals in this industry, especially investigative journalists, are under constant threat (in certain countries) because of their work. Whether their work focuses on corruption in government or ties to organised crime, their work makes them prime targets for attacks by the criminals and corrupt politicians which they seek to expose.

Statistics

A study by the Geneva Declaration on armed violence and development titled *Global Burden of Armed Violence* includes a chapter that tries to apply a quantitative approach to measuring the affects of "intentional homicide" (as they refer to murder) and the number of intentional homicides that occur each year.² The report admits that statistics on intentional homicide rarely capture the number of actual criminal events that have occurred since these crimes can be reported by relatives and witnesses, but obviously cannot be measured through reports by victims. Statistics should therefore be assumed to be conservative estimates. The latest statistics in that study are from 2004 and it estimates that the world average is 7.6 homicides per 100,000 of the population.³

Murders - by Country

Country	Murders
1 Brazil	43,909
2 India	40,752
3 Mexico	20,585
4 Ethiopia	20,239
5 Indonesia	18,963
6 Nigeria	18,422
7 South Africa	16,834
8 Russian Federation	15,954
9 Columbia	15,459
10 US of America	15,241

Source: UNODC (United Nations Office on Drugs and Crime) 2012

The UNODC produced the 2011 Global Study on Homicide, which is a collection of statistical data covering 207 countries and territories. The Study shows that young men, particularly in Central and South America, the Caribbean and Central and Southern Africa, are at greatest risk of falling victim to intentional homicide but that women are at greatest risk of murder owing to domestic violence. There is evidence of rising homicide rates in Central America and the Caribbean, which are "near crisis point" according to the Study. Firearms are behind rising murder rates in those regions, where almost three quarters of all homicides are committed with guns, compared to 21% in Europe. Men face a much higher risk of violent death (11.9 per 100,000 persons) than women (2.6 per 100,000 persons), although there are variations between countries and regions. In countries with high murder rates, especially involving firearms, such as in Central

America, 2% of males aged 20 will be killed before they reach the age of 31 - a rate several hundred times higher than that in some parts of Asia. Worldwide, 468,000 homicides occurred in 2010. Some 36% of all homicides take place in Africa, 31% in the Americas, 27% in Asia, 5% in Europe and 1% in Oceania. Honduras had the highest rate per any country covered by the Study at 82.1 per 100,000.⁴

who is convicted of murder may be sentenced to many years in prison, a prison sentence with no possibility of parole, or even the death penalty. The stiff penalties for committing the crime have undoubtedly deterred many murders; however the deep emotions that a murder creates can be seen as an effective tool to Organised Criminal Gangs and Terrorist Groups, whereby no penalty is too great.

Grievous bodily injury is the intentional infliction of a life-threatening injury or serious injury of a person, or on an important organ or limb of another, makes an important organ or limb unusable, makes another permanently unfit for work, infirm or mentally ill, or the badly or permanently disfigurement of the face of another. This is the Swiss law definition, but as there is no global definition, each jurisdiction has its own. The FATF defined grievous bodily injury as a predicate offence for money laundering in their 40 Recommendations.

Historical Background / Context

Few events have the capability of changing the course of human history as do the murders (or assassinations), of highly popular politicians, civil rights leaders or other influential figures. The immediate societal impact such high profile murders create is what separates this crime from others. Hopes for the future can be crushed immediately, uncertainty sets-in instantly and the backlash of such murders can have consequences that last for generations, even outcomes that couldn't be foreseen or expected.

Here are some of the best examples, all great moments and times in World History:

When those in the Roman Senate led by Brutus assassinated Julius Caesar, in 44 BC intent on defending the Republic from in their eyes a dictator, they little expected that a civil war would follow and that they as the conspirators would be defeated and then would rise a new Political dynasty under Caesar's nephew Octavian, who would become the great Augustus, which would mark the end of Rome once and for all as a Republic, but led to its greatest successes as an Imperial Nation.

Fast Forward to The French Revolution in 1789, with the French people rising up against an absolute monarch, King Louis XVI, and the assault on the Bastille and the passage of the Declaration of the Rights of Man and of the Citizen culminating in the founding of a Republic in 1792 with King Louis XVI being executed in 1793. These momentous times led to Wars in Germany, Holland and Belgium and Italy

and brought in Robespierre and virtual dictatorship by the Committee of Public Safety during the Reign of "Terror" from 1793 until 1794 during which between 16,000 and 40,000 people were killed, where this early use of the word was most definitely State sponsored. Not long after the fall of the Jacobins and the execution of Robespierre, Napoleon Bonaparte would come to power in 1799. The modern era has unfolded in the shadow of the French Revolution. Subsequent events that can be traced to the Revolution include the Napoleonic Wars, two separate restorations of monarchy (Bourbon Restoration and July Monarchy), and two additional revolutions (1830 and 1848) as modern France took shape.

Most Notorious Assassinations over last 100 years	
1914	Archduke Franz Ferdinand
1918	Tsar Nicholas II
1922	Irish President Michael Collins
1940	Leo Trotsky, Russian Communist Leader
1948	Mahatma Ghandi
1963	US President J F Kennedy
1968	US Civil Rights Leader Martin Luther King
1968	US Senator R Kennedy
1973	Spanish PM Luis Blanco
1975	Saudi King Faisal
1978	Italian PM Aldo Moro
1979	Lord Louis Mountbatten (Queen's cousin)
1981	Egyptian President Anwar Sadat
1984	Indian PM Indira Ghandi
1986	Swedish PM Olaf Palme
1991	Indian PM Rajiv Ghandi
1993	Sri Lankan President R Premadasa
1995	Israeli PM Yitzhak Rabin
2001	Nepalese King Birendra
2003	Serbian PM Zoran Dindic
2005	Lebanese PM Rafic Hariri
2009	Pakistan PM (Fmr) Benazir Bhutto

Source: Author See Part 2, Section 6 below

On 9 April 1865 General Robert E. Lee, General of the Southern Confederate Army, surrendered to the Union Government of America ending the American Civil War. Four days later President Abraham Lincoln was attending a performance at Ford's Theatre when

John Wilkes Booth, a Confederate sympathizer and an opponent of the abolition of slavery, entered the presidential booth and shot Lincoln in the back of the head. President Lincoln died the next morning. His death had an instantaneous effect on the people in both the Northern and the Southern States. His death deepened the hatred and the vindictive attitudes of the North towards the South which legitimized the rational for the extremist sentiment and actions of the President's party who wanted to punish Southern states after the war. In addition to the Congressional backlash in Washington D.C., Lincoln's assassination had direct and devastating affect on the South's reconstruction process. Many historians argue if Lincoln hadn't been assassinated, the reconstruction process would have been quicker and the oppression of African-Americans may have narrowed greatly. President Abraham Lincoln was the first US President to be assassinated and John F. Kennedy was the last US President to be assassinated. Both assassinations had an equally chilling affect on the American people's psyche and caused great uncertainty.

President J F Kennedy was murdered at a pivotal time in US history. The assassination took place in November 1963, a year after the Cuban Missile Crisis, an event that brought the world near the brink of nuclear disaster. The civil rights movement, led by Martin Luther King Jr had gathered momentum and was meeting fierce resistance, especially in the South. The Kennedy administration was also in the midst of an unprecedented war on organised crime, led by his brother Robert who was the US Attorney General. The President had many enemies, many of whom wanted him dead. There was great confusion during the first hour after President Kennedy was shot. Since the shooting took place at the height of the Cold War, theories started to take form that the US was under attack from the USSR. One of the only people who may have had knowledge of 'why' President Kennedy was assassinated was the alleged assassin himself, Lee Harvey Oswald, who was murdered two days after Kennedy's assassination. To this day, the level of uncertainty of who assassinated President Kennedy still exists, giving birth to conspiracy theories that would plague the US for decades. These difficult times for America's were only compounded with the assassinations of Presidential hopeful, Robert Kennedy and Martin Luther King Jr in 1968.

Whilst the assassinations of Lincoln and Kennedy had an enormous impact on the US psyche, they didn't lead to a dramatic change in events in either the US or beyond.

That can't be said for the assassination of little known

Archduke Francis Ferdinand, heir to the Austro-Hungarian Empire, whose murder triggered more devastation and loss of life than any before it or since. In June of 1914, Archduke Ferdinand was killed by an assassin's bullet in Sarajevo. Austria-Hungary was searching for a reason to launch a pre-emptive war against Serbia and with the assassination of Archduke Ferdinand, Austria-Hungary was able to secure the promise from Germany that it would aid in a war with Serbia. Due to the existing treaties between the global powers at the time, Austria-Hungary's declaration of war caused a chain reaction that pulled every global power into the First World War. As a result, over 9 million military personnel lost their lives and over 20 million were wounded. The number of civilians who lost their lives has been estimated to be over 6 million. The First World War precipitated the Russian Revolution in 1917 and the execution of the Tsar Nicholas II, leading to the rise of Lenin and the Bolsheviks, then Stalin in Russia and the Soviet Republics and Mao later in China. Of course the end of the First World War and the terms for German Surrender fed German support for Adolf Hitler and the Nazi's leading to World War 2, where many more millions of lives were lost, and would lead historians to conclude that the Twentieth Century was easily the bloodiest in time immemorial.

Whilst death is of course the most severe injury that can be meted out, other punishments and bodily injuries can cause great harm and have significant effects.

Whilst many organised criminal groups have their own modus operandi, many are based on or reflect traditional state sponsored forms of punishment, for example, the so called Five punishments in China date back to ancient times, and included: tattooing, cutting off the nose, amputation of one or both feet, castration and of course death. Later these changed to penal servitude, banishment, death, or corporal punishment in the form of whipping with bamboo strips or flogging with a stick. Fines could also be administered in addition. For women, they could be forced to grind grain, have their fingers squeezed between sticks, be beaten with wooden staves, sequestration or confinement to a room and to be given permission to commit suicide.

When it comes to death, man has tried many ways, many of them vying to be the most gruesome, many state sponsored including Beheading, Stoning, Boiling Alive, Hanging, Hung Drawn and Quartering, Burning, Crucifixion, Garrotting, Drowning, Electrocution, being Shot, Blown Up and or Poisoning which are copied in various ways by organised crime gangs.

Beyond these most final of punishments, Mutilations and various forms of punishment beatings are commonplace with some gangs having very specific modus operandi, for example the IRA, engage in kneecapping, which is where several men force one individual to the ground and set about him. His legs and arms are held taut, the knees smashed by repeated blows, or else a gunman shoots the pinned victim through the kneecaps, perhaps also the elbows. Occasionally the legs have to be amputated.

Victims are beaten or shot in front of their families, dragged into alley-ways, snatched off the street into passing cars.

Money Laundering

Whilst terror organisations will employ murder as part of their raison d'être so would organised criminal gangs who also may carry out attacks on public officials, community leaders or journalists, perhaps under an illegal contract to carry out the attack. These individuals are referred to as "Contract Killers". The illegal contract is usually given to local criminals who are then compensated with cash. The prices for contract killers varies from some of the cheapest in India and Mexico from US\$35 to, for example, US\$700,000 paid to three ex-soldiers to murder a US DEA agent.

Beyond terrorist organisations and organised crime, there are State sponsors of murder with examples such as was the case of Slobodan Milosevic who ordered the assassination of Serbian President Ivan Stambolic by Special Operations Unit officers and the case of Abdurahman Alamoudi who was contracted to kill the Saudi Crown Prince Abdullah by Colonel Gaddafi of Libya. Of course, many of the dictators described as kleptocrats were also involved in the state sponsorship of murder.

Augusto Pinochet, one of the most corrupt and most prominent money launderers in South America's history was eventually placed under arrest because of allegations of murder rather than of corruption or money laundering. This did lead to the identification of a network of accounts and other assets held at a number of US financial institutions particularly Riggs Bank. The investigation found at least US\$27mio had been illegally obtained and transferred through a network of trust funds and shell corporations.

Organised Crime

"Criminals are motivated by profit: so let us go after their money."

Antonio Maria Costa, Executive Director, United Nations Office on Drugs and Crime in 2010¹

This is a popular refrain which has been at the forefront of global policies to defeat organised crime for more than 20 years. Mr. Costa, also stated that "We must increase the risks and lower the incentives that enable the bloody hand of organised crime to manipulate the invisible hand of competition"

After Osama bin Laden was killed in 2011, the head of an organised criminal gang became the most wanted man in the world. Joaquín Guzmán Loera (El Chapo) is the leader of the Mexican Sinaloa Cartel, that controls a significant part of the drug trade into the US who also earned the title as "the world's most powerful drug trafficker." Whilst the Sinaloa Cartel jealously and violently defends its interests it both competes and works with other Organised Gangs both in Mexico and around the world. The existence of Organised criminal gangs on every continent in virtually every country remains a significant threat to society.

Harms

Organised crime is considered as one of the major threats to society, both in threatening citizens physical security and in the pursuit of serious crimes which undermine legitimate business, corrupt political and legal structures and in so doing undermine the development of and effective functioning of societies worldwide.

Statistics

According to the UNODC Report issued in October 2011, money flows related to transnational organised crime activities represented approximately US\$870bio the equivalent of some 1.5% of Global GDP, 70% which or 1% of Global GDP or US\$580bio is thought to have been available for laundering through the financial system. The largest income for transnational organised crime comes from illicit drugs, accounting for a fifth of all crime proceeds. According to UK authorities,² the total cost of the social and economic harm caused to the UK by serious organised crime is in the region of £30bio a year. Its victims range from those whose lives are ruined by drug addiction, to women who are trafficked for sexual exploitation, to businesses who suffer losses from fraud or are forced to close in the face of illegal competition.

In Italy, organised crime generates up to US\$204bio (turnover) every year according to Conteserati (Italian Employers' Federation) also stated the Italian Mafia has US\$83bio in liquidity. Around 270,000 businesses in the country associated with the Federation reported being subjected to 1,300 crimes a day by organised crime gangs

Definition / Description

Organised crime gangs come in different shapes and sizes, appearing in many forms at different times and in different places, exerting different levels of organisation, geographic coverage and criminal focus. According to the US Organised Crime Control Act 1970, Organised crime is the "unlawful activities of a highly organised, disciplined organisation," and according to the UN Convention against Transnational Organised Crime 2000 (the Palermo Convention) a "structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences, in order to obtain directly or indirectly, a financial or other material benefit.³ According to the UNODC, transnational organised crime largely focus on the trafficking of drugs, in persons (including for sexual exploitation), smuggling of firearms, trafficking of natural resources (such as timber, and wildlife, including elephant ivory, rhino horn and tiger parts, product counterfeiting (including counterfeiting of medicines) maritime piracy and cyber crime. Whilst their activities are illegal they do in large part respond to a reasonably large demand for certain services from parts of the community. As globalization has expanded international trade, so the range of organised criminal activities has broadened and diversified to whatever makes them money or where they can gain influence or control. Today's leading organised criminal gangs operate internationally and often with each other, though great enmities and rivalries exist too. Organised Criminal Gangs operate using the clear threat of violence and incentives, also corruption as a persuasive technique both to ensure order within the Gang but also to encourage third party compliance or support when appropriate.

As Organised criminal gangs generate so much money, they need to launder this money on an industrial scale and invest time and effort into disguising and converting it into funds that are then available for investment into legitimate enterprises or into valuable assets that are not traceable back to the original criminal proceeds. The gangs will use violence and the threat of violence and incentives including bribery as persuasive techniques both to ensure order in the gangs but also to protect and to expand their operations.

Historical Background / Context

The term "organised crime" appears to have emerged in Chicago in 1919, gaining traction through the era of prohibition and through the exploits and ultimate demise of one of the Worlds most notorious criminals, Al Capone. But the phenomenon of organised criminal activity far pre-dates this and its manifestations have developed considerably since that time. One of the first recorded were "thugs" or gangs of criminals, who terrorised 13th century India moving from town to town, looting and pillaging and of course later in the piracy on the high seas, highwaymen and banditry were to the pre-industrial world what organised crime is to modern society. Many of today's leading organised criminal gangs also have long histories, many tracing their origins back to feudal times, retaining links and codes from a bygone era whilst at the same time modernizing and expanding their operations far beyond their traditional roots from their homelands across the world.

Money Laundering

Money Laundering theory, based on largely studying Organised criminal activity, suggests that as OC groups generate very large amounts of money, this money becomes much more valuable to them if they can disguise it and convert it into funds that are available for investment into legitimate enterprises or into valuable assets that are not traceable back to the original criminal proceeds. Money Laundering is a three-stage process: Placement: (also called immersion), generally inserting crime funds into the legitimate financial system; Layering: disguising the trail of the monies as they pass through the financial system, so the monies cannot be linked to criminal proceeds and also called 'heavy soaping' and finally Integration (also called 'spin dry'), when the funds make it into legitimate income or assets. As many of the leading organised criminal gangs are involved in a material way in drug trafficking, and indeed many have made their names and branched out following success in trafficking drugs, the methods and networks used by these organised criminal gangs will be largely those used by those drug traffickers.

OCs will use Banks and other Financial Institutions for all manner of services including moving, using and storing and other non-Bank operators such as, for example, Money Services Businesses as well as informal channels such as unregulated money transfer systems, non-financial operators, such as cash intensive businesses, for example, Casinos or retail outlets to launder monies and others such as Real Estate Agents, Precious Metal Dealers and High Value Goods Dealers in items like, Art, Planes, Boats and Cars.

Examples of particular Banking services that are particularly attractive to support organised criminal activity, include of course Private Banking services. This service is attractive in order to manage significant criminal proceeds for investment or privacy purposes usually via various front companies, trusts or foundations established by specialists, for example Lawyers, Fiduciaries and Company Service Providers.

Another service is the cash, cheque and other payment services offered by Banks that enable OC Gangs to move and launder their money, sometimes over great distances internationally, via Correspondent Banking. Good examples would be the cases of Lucy Edwards and Peter Berlin which led to criticism at the Bank of New York, Pedro Allatore working at Casa De Cambio Puebla in Mexico City helping one of the Mexican Drug Cartels launder money via Wachovia Bank and through HSBC.

Money Services Businesses are a frequent target for OC gangs trying to launder money, with Beacon Hill and Lespan as well as Sigue Corporation also good examples. As are Precious Metals and Stones Dealers, with La Mina and Operation Polar Cap and Speed Joyeros very good examples.

A favourite method used in particular by Drug Trafficking Organisations is the Black Market Peso Exchange utilised by the Colombian Cartels as a trade base money laundering system. For details see Drug Trafficking and Smuggling above.

Organised Crime, including gangs, will also smuggle cash. For details see "Smuggling" below.

When it comes to the use of Cash Intensive Businesses few were more useful than Casinos, with the Italian American Mafia sending Bugsy Malone to Las Vegas to establish their first Casino. The Italian American Mafia like many other Organised Criminal Gangs have used many front businesses to launder cash, with cash generating businesses popular, with perhaps the best example being Al Dente's Pizzeria in New York City which was raided by the FBI following the undercover work of the real Donny Brasco and which case became known as the Pizza Connection.

Organised Criminal gangs can be found in most countries in the world with the most successful exploiting key points of interest along the value chain of the most profitable criminal industries whether drugs, people or products and in origin transit and destination countries. Concentrations do appear in many of the Worlds largest and most successful Countries and Cities,

where trade, demand and opportunities abound.

There are no government published lists covering the Worlds Organised criminal gangs, nor are there many rankings of organised criminal gangs where membership size, success in generating proceeds, harms caused etc are collected and made available, though there are many private publications relating to one or more gangs and a number of authors that have tried to collect information on some of the most important. One ranking list was identified as follows:

10 Most Dangerous Gangs in the World	
1	Mara Salvatrucha (MS-13)
2	Latin Kings
3	Aryan Brotherhood
4	Los Zetas
5	18th Street Gang
6	Bloods
7	Yakuza
8	Wah Ching
9	Crips
10	Cosa Nostra

Source: Wiki, National Geographic⁴

The following is a brief summary of the regions and key countries in the world where Organised crime is a significant threat and highlights the most important Organised criminal gangs known to be operating. The gangs and groups include mafia type organisations, street gangs, prison gangs and other gangs that are involved in substantial collective criminality. Profiles for these and other Organised Criminal Gangs are set out in Part 2, Section 5, Criminals & Terrorists.

Africa

Africa is home to only a number of major organised criminal gangs, including the People Against Gangsterism and Drugs and the Numbers Gang in South Africa, the Mungiki in Kenya and in Nigeria, the Nigerian 419 and other Fraud gangs and the Area Boys. The lack of organised criminal gangs, compared to other regions is probably a result of limited opportunities, tribal allegiances and state domination in much of Africa.

Middle East

With the continued struggles and conflict in the Middle East and the number of terrorist organisations calling the Middle East home, organised crime is largely

crowded out or otherwise its these groups that can be considered organised criminal gangs. Classic organised criminal gangs can be found still in Israel, for example, the Abergil Crime Family, the Alperon Crime Family and the Zeev Rosenstein Organisation. And in Turkey for example, the Turkish Mafia and the Ulkucu Hareket.

Golden Crescent

In the region known as the Golden Crescent, in particular centred on opium production in Afghanistan and in neighboring Pakistan, Afghan Warlords still operate, one such group is the Afriди Network but also of note is the Khan Cartel and the Haqqani Network. Of course many of the terrorist organisations in the region including the Taliban also operate as organised criminal groups to fund their activities.

India/Pakistan

In India and Pakistan, the D Company is the most significant of the organised criminal gangs. In Mumbai D Company has competition from Chhota Rajan, Arun Gawli, Late Amar Naik and Chhota Shakeel.

Asia

Golden Triangle

In South East Asia, the area in and around the Golden Triangle, (Thailand, Myanmar and Laos) is particularly attractive to organised criminal gangs as an area that produces large amounts of heroin, including the Khun Sa cartel (see also Mong Tai Army); and the United Wa State Army; The Red Wa operate in Myanmar and originally part of the Burmese Community Party's military. Jao/Chao Pho are ethnic Chinese gangs in Thailand. In the Philippines they have become the second largest producers of Marijuana in the world after Mexico and an important transit point for other drugs in the region and so alliances have been formed that involve the 14K Triad, the United Bamboo, the Heavenly Alliance and the Four Seas gang all of Taiwan, the Big Circle Boys and the Yakuza.

China

In China, the Triads, whose history may go back as much as 2000 years, played a major role in the Chiang Kai-shek regime gradually increasing the scope of their criminal activities, but they were enemies of the Communists and had to flee after the Communists came to power in 1949. The Triads left settling mostly in Hong Kong, but also Macau and in Taiwan and also represented in countries with significant Chinese populations, such as Malaysia, Singapore, the US, Canada, Australia and the UK. There are around 50 known triad societies in Hong Kong alone, the main ones being the Sun Yee On and 14K which are the two

largest and well known but other large gangs include Wo Shing Wo, Wo Hop To and Wo On Lok, are also important. In Taiwan, the United Bamboo is believed to be Taiwan's top Triad gang. Other Taiwanese gangs include Heijin, Heavenly Alliance and the Four Seas. The Dai Huen Jai are not a Triad gang but a Chinese criminal gang and the Tongs are similar to triads except that they originated among early immigrant Chinatown communities independently, rather than as extensions of modern triads.

In Oceania, organised crime has focussed its attentions on the regional economic power of Australia but also New Zealand. Gangs in Australia often form on ethnic lines, and there are Chinese Triads, Japanese Yakuza and Vietnamese gangs, but also include Lebanese, Italian, Romanian and even Colombian Syndicates. Of the Triad groups the 14K is well established in Sydney with branches in the other major cities. Also active are the Big Circle syndicate. In Melbourne as well as those already mentioned are the Sun Yee On and the Wo Yee Tong and the Wo Shing Wo. The latter two are sub-groups of the Wo Group. Outlaw motorcycle gangs are present in Australia, with international outlaw clubs like the Bandidos and Hells Angels and Gypsy Joker as well as locals such as the Coffin Cheaters, the Comanchero, the Nomads, the Notorious and the largest the Rebels. Youth Gangs have flourished throughout many of the large cities of Australia, especially Melbourne and Sydney, but also more recently throughout the outer suburbs of Brisbane as well. There have also been a few cases of Australian gangs imitating American street gangs such as the Bloods, including gangs such as Butch Lesbian Soldiers (BLS), Village People and FLC.

In New Zealand organised crime is largely carried out by motor cycle and street gangs, and criminal elements of the Asian community. The Hells Angels (Auckland) was in fact the first chapter established outside California (1961). Also two other US groups, The Bandidos and the Outlaws also have interests on the Islands. The Asian community in New Zealand has increased dramatically in the last decade as a result of increased immigration and has unwittingly brought with it gangs such as 14K, Sun Yee On and the Wo groups. Other groups emanate from Thailand, Vietnam, Malaysia, Singapore and Japan. The Maoris have also formed organised gangs with the most important being The Mongrel Mob, Black Power and Nomad gangs.

Japan

In Japan, the Yakuza dominates through its main syndicates, the Yamaguchi-gumi; the Sumiyoshi-kai; the Inagawa-kai; the Dojin-kai; and the Kyushu Seido-kai.

Americas

The US and Mexico are homes to some of the worst organised crime problems in the world. The contiguous land border between the two has enabled a significant flow of criminal activity between the two states and organised crime is increasingly penetrating the legitimate business world for both laundering purposes and the movement of merchandise with illicit products hidden within. Canada has also been effected, by its proximity to the US and by its relatively open border.

United States of America

Whilst we are all familiar with the Prohibition era in the US when the fame of gangsters such as Al Capone and Bugsy Malone grew, and since, as Hollywood has portrayed these times as particularly dangerous, the problems of organised crime are today much worse. Al Capone's Chicago has also to a large degree been superseded by New York, Los Angeles, Dallas and Miami not only because of their local mobs but because they are key entry points for the drugs and cash in need of laundering, arriving from Latin America and South East Asia. Whilst classic organised criminal gangs such as the Italian American Mafia, in particularly La Cosa Nostra remain, though much less powerful after continued targeting and successful prosecutions, and the rise of new competitors, they do remain still important, particularly in some Eastern Seaboard cities. They include such groups as the Bonanno, Colombo, DeCavalcante, Gambino, Genovese and Luchese families. The other Italian Mafia groups are also present in the US though not as significant, including the Comora, the Ndranghetta and the Sacra Corona Unita.

The landscape has changed however and the one that exists today includes many important players, including street gangs, prison gangs and other gangs that work closely with Mexican and other foreign organised criminal gangs to supply illegal drugs and other goods and services to the worlds biggest and most wealthy market. Mexican's as well as South American Gangs, including the Colombians as well as Japanese Yakuza and the Chinese Triads, the Russian Mafia and Albanian Mafia as well as home grown Outlaw Motorcycle Gangs. The Triads are considered a major problem, with close 'business' links to the Mafia, they flourish in the 'Chinatowns' of San Francisco, Los Angeles, Portland, Denver, Houston, Phoenix, Chicago, Boston Philadelphia, Atlantic City and New York. As well as the usual crimes it is estimated that with their Hong Kong and Taiwanese links the Triads are responsible for much of the world's forged credit cards. They are also connected to violent street gangs such as the 'Ghost Shadows' or 'Flying Dragons'. The Japanese Yakuza are prominent in Hawaii with significant holdings

in real estate. Jamaican Posses are involved in Drugs distribution as are Nigerians who use a route from Latin America through West Africa to then bring drugs into both Europe and North America.

Perhaps the most troubling though of all the developments is the rise of Russian and Eastern European including the Russian Mafia, Chechen Mafia and Albanian Mafia who are involved in tax and health care fraud, alien smuggling, extortion, drugs, and of course money laundering. As many of these started out in contract killing they are particularly violent groups, with little regard for traditional gangland rules.

Much of the proceeds of crime are generated in cash and a wide variety of methods is used by gangs to launder the money. Much is hidden until it can be smuggled out to another destination where it can be released into the local economy. Increased use is also being made of the casa de cambios of Latin America, the Hui Kwan and Chop Houses of East Asia / Hong-Kong and the Hawala and Hundi systems of South Asia and Middle East. The non-bank system includes insurers, mortgagees, trading companies, gold and precious metal dealers, cheque cashing services express delivery services, etc. Wire transfers can hide criminal proceeds in the vast numbers and amounts going through the financial system and as such is one of the most important instruments for layering illegal proceeds in terms of the volume of money that can be moved and the extent to which transfers occur.

Clearly the US, in a global economy, is facing the globalisation of crime and criminal organisations. Its northerly neighbour Canada and its southerly neighbour Mexico are integral to this global criminal economy, which are part of, as well as being under attack from, foreign criminal groups that easily rival the inheritors of the American mobster. Beyond the classic organised crime gangs lies a more dangerous phenomena, being the American Street and Prison Gangs. Approximately 1.4 million active street, prison gang members, comprising more than 33,000 gangs, are criminally active within the USA. This represents a 40% increase from an estimated 1 million gang members in 2009, with Arizona, California, and Illinois with the highest number of gang members.

The main Prison Gangs in the US are the Aryan Brotherhood, Mexican Mafia, La Nuestra Familia and the Texas Syndicate.

The most notorious American street gangs have been formed from the streets of major cities like Los Angeles, which have spawned the Crips and the Bloods, Mara Salvatrucha -13 or MS-13 and the 18th Street Gang, the

Latin Kings and Wah Ching, and the Black Guerrilla Family (Black Family, Black Vanguard).

Whilst the Hell's Angels are the best known of all the so called "Outlaw Motorcycle Gangs", the Outlaws, the Bandidos and the Pagans, make up the top 4 biker gangs with other gangs the Mongols, the Vagos Motorcycle Club and the Wheels of Soul, each of which stake claim to territory in North America, and in Europe, particularly in the UK, Scandinavia and elsewhere, even in Australia. Membership is as high as 44,000 in the US with approximately 3,000 gangs or sub gangs in total.

Of the far right groups in the US the Ku Klux Klan still remains the most notable.

Mexico

Mexico's geographical position set between the world's largest cocaine producers and one of the world's biggest consumers of cocaine making it a logical transit route for the product. Mexican Drug Trafficking Organisations (DTOs) are essentially transport and logistics organisations who are competing for the business of supplying the US with marijuana and cocaine supplied by indigenous, Central American and South American producers, and, in the case of Ephedra based products; China.

The DTOs are located in specific geographic areas within Mexico. The Cartels are located in those areas along Mexico's border with the US and in its Gulf, Caribbean and Pacific ports. Some are also located on the connecting highway routes between these points.

Mexican criminal gangs include the Sinaloa Cartel, Los Zetas, Gulf Cartel, Tijuana Cartel, Beltrán Leyva Cartel, Juarez Cartel and the Knights Templar Cartel, each control large swaths of Mexican territory and dozens of municipalities. There were no cartels in the 1980s in Mexico, as the entire business was controlled by one man, Félix Gallardo who was known as the "Godfather".

The cartels are currently waging violent turf battles over control of key smuggling corridors through Mexico and defending themselves from government action. The Sinaloa cartel is considered the largest and most powerful drug trafficking organisation in the world and fugitive Joaquín Archivaldo Guzmán Loera is its leader. Known as "El Chapo Guzmán" ("Shorty Guzmán") for his 1.68m (5ft 6in) stature, he became Mexico's top drug kingpin in 2003 and is now considered, "the most powerful drug trafficker in the world," by the US Department of the Treasury. Los Zetas is considered the

most violent.

Mexican cartels are also increasing their relationships with prison and street gangs in the US in order to push market distribution. A US Congressional report noted that gangs such as the Latin Kings and Mara Salvatrucha (MS-13) buy bulk methamphetamine from Mexican drug cartels for resale. Again, according to the FBI, Mexican cartels focus only on wholesale distribution, leaving retail sales of drugs to the street gangs. The cartels will sell to all and any gangs but do not take sides in US gang turf wars.

Caribbean

Of the 16 countries in the Caribbean area four have been identified by President Obama as major drug producing or transit countries. These are Haiti and the Dominican Republic, the Bahamas and Jamaica.

Jamaica

Jamaican organised crime is the most powerful in the region and is present in the cities of the US, Canada and the UK and Canada. The major crime groups are deeply involved in the international drug trade and within Jamaica protection rackets and extortion. They have penetrated the formal economy in both legitimate and illegitimate businesses. They have massive political influence with corruption endemic. The Posse's as they are known in the Americas or Yardies as they are known in the UK are loose groupings of gangs first became involved in drugs and gun-running in the early 1980s and have been described by some as an example of organised disorganised criminals. The most well known is the Shower Posse.

Central America

Central America consists of the seven states of Belize, Honduras, Guatemala, Costa Rica, Nicaragua, and El Salvador with a combined area smaller than Texas. Today organised drug crime has increased its already substantial presence and widened its activities. It is now the main cause of the bloodshed within Central America which is used as a bridge between Colombia and Mexico and from there onwards to the US.

These problems are even more acute in the so called Northern Triangle of Guatemala, El Salvador and Honduras.

Indigenous gangs have existed for decades moving drugs, contraband, humans, and arms but now the Mexican Cartels have moved in as drug flights from South America into Mexico becomes more difficult and seaborne interdiction more effective on the Caribbean and Pacific routes into Mexico and the US.

Most of the organisations that participate in drug trafficking in the Northern Triangle are tasked primarily with the protection and transportation of Colombian or Mexican-owned products. One example of this relationship is the Mexican Sinaloa Cartel's links with Los Perrones Orientales, an organised crime group that transports product by land from the Pacific Coast to Guatemala. Another part of the organised crime structures are youth gangs. There is evidence that the upper echelons of transnational youth gangs, such as the Mara Salvatrucha (MS13 and MS18), provides security, or "muscle," for the Mexican cartels and frequently provide transport services for organisations like Los Perrones Orientales. These upper levels are often made up of former combatants from former conflicts in the region.

The other main Mexican cartel, Los Zetas are attempting to recruit senior Mara 18 members. They also recruit from the notorious disbanded Guatemalan Special Forces known as the Kabilas. Mara 18 is the local name of the 18th Street Gang that originated in Los Angeles in the US and came to the region when gang members were deported from the US back to Central America. There are an estimated 70,000 maras in Central America. These youth gangs are a ready supply of willing teenagers who can ferry drugs, look after kidnap victims and carry out other low-level crimes although they run large scale protection racket.

South America

Of all the Countries of South America Brazil, Colombia and Venezuela have the biggest problems with organised Crime.

Brazil

In Brazil criminal gangs are dispersed and usually based on the favelas with control being exercised by the use of terror. The organisations are directed exclusively at the business of drugs and weapons. Unfortunately this is not all as some sectors of the various Policing groupings are accomplices of organised crime. In Rio de Janeiro, the Blue Command and the Red Command can be found and in São Paulo a group known as PCC or First Capital Command dominates the massively overcrowded prisons and is also a significant threat outside.

Colombia

Colombia has long epitomized drug cartels and decades long terrorist/insurgent struggles. The Country is home to terrorist groups such as FARC, the ELN and the AUC, although the AUC has been largely disbanded although some are said to have reformed or even become part of the Colombian Government forces.

These groups also operate in ways similar to those involved in organised crime. Colombia remains the world's leading producer of cocaine, controlled by the Colombian Drug Cartels. In the late 1990s and into the first decade of the twenty first century, three-quarters of the world's annual yield of cocaine was produced in Colombia, both from cocaine base imported from Peru and Bolivia, and from locally grown coca.

The Colombian Drug Cartels are criminal organisations developed with the primary purpose of promoting and controlling drug trafficking operations. During the 1980s, as demand for cocaine increased, existing Colombian Drug Cartels expanded and organised into major criminal conglomerates usually headed by one or several kingpins as in the case of the Medellin Cartel led by Pablo Escobar and the North Coast Cartel, led by Alberto Orlandez-Gamboa "Caracol" (the snail) along with federation-style groups such as the Cali Cartel (founded by the Rodríguez Orejuela brothers, Gilberto and Miguel, as well as associate José Santacruz Londoño) and the Norte del Valle Cartel (Founded by Diego León Montoya Sánchez, Wilber Varela and Juan Carlos Ramírez Abadía).

With the collapse of many of these major Cartels, a new organisation, Norte del Valle Cartel, became established and inherited much of the drug trafficking operations, though the establishment of a military wing and infighting have produced "Los Rastrojos" as one of the most important drug trafficking groups in Colombia and beyond. Other Cartels, albeit not as powerful, do exist including the Cartels in Bogota, Caqueta, and Llano, as well as more than 300 additional drug smuggling organisations or 'Cartelita's' (baby cartels).

Other organisations in Colombia are also involved in drug trafficking including paramilitary or terrorist groups which use the provides of drug trafficking to finance their activities. These include the AUC, Black Eagles, ELN, FARC, ERPAC, Oficina de Envigado, Los Paisas and Los Urabeños. All the groups currently running the country's drug trade are known collectively by the government as "criminal bands," or BACRIMs

Venezuela

Venezuela's long porous borders with Colombia and Brazil and an island dotted coastline facing the Caribbean Islands has made it a major player in the illicit drugs industry. Whilst Colombian gangs have long since operated in Venezuela, often dominating organised criminal activity, and having a permanent presence in the cases of both the Revolutionary Armed Forces of Colombia (FARC) and the National Liberation Army (ELN), just as Mexicans have eclipsed

their Colombian criminal counterparts over the last decade, there is evidence that Venezuelans are moving in the same direction. For example whilst the Colombians traditionally controlled the flow of cocaine through Venezuela to organisations in Mexico and Europe, they are being replaced by Venezuelan gangs who buy cocaine as it crosses the border then sell it on to transnational criminal organisations, principally the Mexicans, but also the Italian Mafia. Evidence suggests that most of the Venezuelan gangs have ties to, or are directed by, members of the Venezuelan military. The term "Cartel of the Suns" (Cartel de los Soles) is used to describe groups inside Venezuela's military that traffic cocaine.

Eastern Europe

Eastern European gangs include the Russian Mafia including the Solntsevskaya Bratva in Moscow and the Tambov Syndicate in St Petersburg, the Chechen Mafia including the Obshina and the Albanian Mafia, for example Nono Aldo Bare, the Serbian Mafias, and the Pruszkow Mafia in Poland.

Western Europe

Western Europe is home to numerous organised criminal gangs including probably the most infamous of them all, the Mafia in Italy, including the Cosa Nostra in Sicily, the Comorra in Naples, the Ndrangheta in Calabria and the Sacra Corona Unit in Puglia. In the Netherlands, the Bruinsma Drug gang operate, in France, there is the Corsican Mafia and the Horne Gang, in Sweden the Original Gangsters and the Uppsala Mafia and Black Cobra, in Denmark. In the UK the Clerkenwell Crime Syndicate also known as the Adams Family and Curtis Warren, and in Ireland the Gilligan Gang and the Foley Gang.

For more details see Part 2, Section 5, Regions, Countries, Criminals & Terrorists.

Smuggling

"Smuggling organisations are opportunistic and for the right price could knowingly or even unknowingly use their smuggling techniques, routes and methods to smuggle dangerous criminals, weapons, drugs, contraband or worse into this country."

Brian Moskowitz, US Immigration and Customs Enforcement (ICE)¹

Harms

Smuggling severely harms the economy of a country in multidimensional ways. It undermines the local industry, discourages legal imports and reduces the volume of revenues collected from duties and levies by the state. Unfortunately smuggling reaps huge benefits for criminal organisations and terrorists alike. In a report released by the World Customs Report, titled Tobacco and Cigarette Smuggling, it was determined in the case where goods are highly taxed, easily portable and penalties remain relatively light for smuggling, transnational criminal organisations will take advantage of any weaknesses in customs, revenue or other border controls to amass profits.²

Not only is smuggling illegal but certain types such as trafficking for the purpose of modern day slavery or sexual exploitation is also a crime against humanity.

Statistics

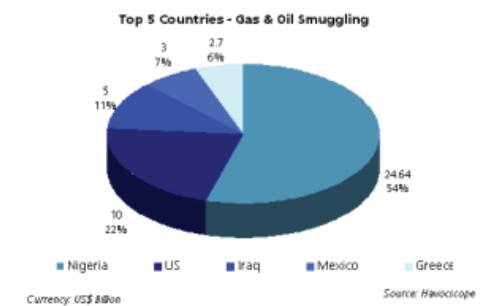
According to Havocscope, the Top 5 Smuggling activities are as follows:³ smuggling, which can take the form of alcohol (US\$5bio), cigarettes (US\$50bio), oil and gas (US\$37.25bio) as well as wildlife (US\$19-32bio), metals and minerals (US\$2.3bio), nuclear smuggling (US\$100mio) and human smuggling (US\$35bio), could amount to almost US\$1.62bio. Nevertheless, wildlife smuggling could be more appropriately included in Environmental Crime and human smuggling in Human Trafficking. Without these, smuggling estimates fall to US\$95bio. This ranks it fourth or fifth as a result in overall black market activities depending upon which is included.

Gas & Oil

In June 2012, officials with oil companies and the Nigerian Government reported that over US\$1bio in oil revenue were being lost to the oil being stolen. In 5 months, security services in Nigeria shut down over 900 illegal oil refineries across the country.⁴ Reuters reported that a legislative committee estimated the annual revenue loss in Nigeria due to the black market smuggling of fuel was US\$4bio.

According to the Maritime Industry Advocacy Initiative in 2011, 600,000 barrels of oil is being lost in Nigeria each year, which puts the annual losses to oil smuggling at around US\$24.6bio. In 2011, the Mexican government-controlled oil producer Pemex reported losing 3.35 million barrels of fuel to oil smugglers. In

2010, the company lost 2.16 million barrels of fuel. The estimated losses for the company in revenue to oil theft and smuggling is around US\$1bio. The oil theft has a severe impact on Mexico's federal budget, as profits from Pemex pays for one-third of the government's federal budget.⁵ The Top 5 Countries for Gas and Oil smuggling are as follows:⁶



Cigarettes

Cigarette smuggling causes US\$50bio in lost tax revenue to governments around the world, according to the World Health Organisation in March 2012. At least 10% of all cigarettes sold in the world were smuggled on to the black market.

In 2011, an estimated 65 billion cigarettes were smoked in the EU that were smuggled and purchased on the black market. The black market cigarettes caused a loss of tax revenue of US\$1.2bio for the EU budget and up to US\$11bio in lost tax revenue for EU member states.

In New York City, where the combined state-local tax rate is US\$5.85 a pack, up to US\$40mio a year in tax revenue is lost to cigarette smuggling. A NYC wide sweep of 1,700 stores licensed to sell cigarettes found that 42% of stores were either selling untaxed cigarettes or packs of cigarettes with counterfeit tax stamps on them.⁷

A similar annual estimate for losses was provided when the head of a domestic cigarette manufacturer in Jamaica said that cigarette smuggling in the country causes the government to lose between US\$34mio and US\$45mio.⁸

The Government of Greece loses up to US\$654mio to cigarette smuggling activities each year as 170mio black market cigarette packs are sold within the country.

Wildlife Smuggling and Poaching

According to Europol, the trafficking of endangered species is worth US\$32bio, with the EU being the foremost destination for these species and Europol and Interpol involved in countering this trade.⁹

Endangered Animals & Wildlife Prices	
Arowana Fish	US\$20,000
Baby Elephant in Thailand	US\$7,000
Baby Tiger in Iran	US\$3,200
Bear Bile	US\$200,000 per pound
Black Cockatoo	US\$31,000 in Australia
Clouded Leopard	US\$5,700 in China
Elephant	US\$28,200
Elephant Tusk	US\$1,800 in Vietnam
Full Dead Bear	US\$2,500 in Taiwan
Geckos from New Zealand	US\$1,300 in Europe
Gorillas	US\$40,000
Iguanas	US\$10,600
Ivory	US\$1,800 per kilo
Komodo Dragon	US\$30,000
Orangutan	US\$45,000
Ploughshare Tortoise	US\$4,000
Polar Bear Skin	US\$7,760 - US\$9,930
Rhino Horn Dagger	US\$14,000
Rhino Horns	US\$97,000 per kilogram
Shark Fins	US\$400 per pound
Snake Venom	US\$215,175 per litre
Snakes (Banded Kraits)	US\$2,190 in India
Snow Leopard Pelt	US\$1,000 in Afghanistan
Tiger (Dead)	US\$5,000
Tiger (Live)	US\$50,000
Tiger Remains	US\$70,000 in China
Tiger Skin	US\$35,000
Tortoises	US\$10,000 in Madagascar
Turtle	US\$20,000 in China

Source: Havocscope¹⁰

The World Wildlife Fund (WWF) estimated the global illegal trade in Wildlife as worth US\$19bio, much of which is used to finance criminal conflicts.

Alcohol

BBC News reported in 2011 that alcohol smuggling leads to US\$1.6bio in lost tax revenue to the UK government. The illicit sales of spirits alone causes US\$490mio in tax revenue losses.¹¹ Frontline reported in 2007 that alcohol smuggling in Iran brings in

US\$2.5mio a day.¹² The Industry Association for Responsible Alcohol Use reported that alcohol smuggling in Canada causes losses of US\$734mio every year.¹³

Top 10 Countries – Alcohol Smuggling		
1	UK	US\$1.6bio
2	Iran	US\$912.5mio
3	Canada	US\$734mio
4	Russia	US\$700mio
5	Thailand	US\$334mio
6	Colombia	US\$300mio
7	Malaysia	US\$268mio
8	Turkey	US\$60mio
9	US	US\$34mio
10	Cambodia	US\$22mio

Source: Havocscope¹⁴

Metals & Minerals

In South Africa, Peru and the Democratic Republic of Congo, illegal gold trafficking creates a yearly loss of US\$2.3bio a year, according to a report by Global Financial Integrity (February 2011).¹⁵

Illegal mining groups in Colombia are reported to be paying 1% of their total production in extortion fees to paramilitary groups such as the FARC, who generate up to US\$1mio a month from illegal mining activities. The Mine Minister of Colombia estimated that at least 40% of all mining activities in Colombia in 2011 were unlicensed.¹⁶ The drug trafficking and paramilitary organisations control at least 30% of the illegal mining activities.¹⁷

Custom officials in India reported seizing 48,600 crates of conflict diamonds in Surat and Mumbai in 2011. The crates of diamonds did not have the proper Kimberly Process Certification and were believed to have been smuggled out of Zimbabwe. The diamonds were worth US\$1.75mio. Up to US\$1bio in potential revenue from the extraction of diamonds in Zimbabwe was reported to be missing as of 2011, according to the country's Finance Minister and civic leaders. 10 out of 11 diamonds sold around the world are cut in India.¹⁸ For more information see Precious Metals & Stones.

Definition / Description

Smuggling is the underground transportation of goods or persons, such as out of a building, into a prison, or across an international border, in violation of applicable laws or other regulations. It also involves the importing or exporting without paying lawful customs charges or duties. Smuggling is also defined as international trade through 'unauthorised route' such as a seaport, airport or land port which has not been authorised by the gov-

ernment for importation and exportation. Smuggling is a cognisable offense in which both the smuggled goods and the goods are punishable.

There are various motivations to smuggle. These include the participation in illegal trade, such as in the drug trade, in illegal immigration or illegal emigration, tax evasion, providing contraband to a prison inmate, or the theft of the items being smuggled.

Historical Background / Content

Smuggling dates back to probably the first time duties were imposed, or any prohibitions were placed on imports or exports. In England it first became a recognised problem in the 13th century, following the creation of a national customs collection system. The export of highly taxed export goods such as wool and hides were smuggled, as well as goods such as grain to circumvent prohibitions or embargoes on particular trades. Imports of wine were also sometimes embargoed during wars to try to deprive the French of the revenues that could be earned from their main export.

Again, taking England as an example, in the mid-16th century, the illicit export of goods like grain and leather represented a significant part of British business, with many members of the civic elite engaging in it. Grain smuggling by members of the civic elite, often working closely with corrupt customs officers, has also been shown to have been prevalent during the later 16th century. Wool was smuggled into England in the 17th century under the pressure of high excise taxes. The high rates of duty levied on tea and also wine and spirits, and other luxury goods coming in from mainland Europe at this time made the illegal import of such goods and the evasion of the duty a highly profitable venture for impoverished fishermen and seafarers. In certain parts of the country, the smuggling industry was more economically significant than legal activities such as farming and fishing. The principal reason for the high duty was the need for the UK government to finance a number of extremely expensive wars with France and the US.

Smuggling in colonial times was a reaction to the heavy taxes and regulations imposed by mercantilist trade policies. After American independence in 1783, smuggling developed at the edges of the US at places like Passamaquoddy Bay, St. Mary's in Georgia, Lake Champlain, and Louisiana. During Thomas Jefferson's embargo of 1807-1809, these same places became the primary places where goods were illegally smuggled out of the nation. Like Britain, a gradual liberalization of trade laws as part of the free trade movement meant less smuggling. In 1907, The Roosevelt Reservation, which was a 60-foot strip of land on the US side of the US-Mexico Border, was established to keep the land "free from obstruction as a protection against the smuggling of goods between the US and Mexico." Smuggling revived in the 1920s during Prohibition, and drug smuggling became a major problem after 1970s. In the 1990s, when economic sanctions were imposed

on Serbia, a large percent of the population lived off smuggling petrol and consumer goods from neighboring countries. The state under President Slobodan Milosevic actually promoted smuggling to fund the wars and to reward Serbian organised crime and Serbian Militias.

In modern times, as many OECD Member countries have struggled to contain a rising influx of immigrants, the smuggling of people across national borders has become a lucrative illegal industry with people-trafficking, especially of women and children effectively enslaved.

Money Laundering

There are various types of smuggling which yield high illegal profits.

Goods

Much smuggling occurs when enterprising criminal merchants attempt to supply demand for a good or service that is illegal or heavily taxed. As a result, illegal drug trafficking, and the smuggling of weapons and humans, as well as the historical staples of smuggling, alcohol and tobacco alongside other highly taxed goods such as Precious Metals & Stones, Wildlife, oil and gas or products used for possible illicit purposes like metals and minerals or cash, are widespread. As the smuggler faces significant risk of civil and criminal penalties if caught, the criminal smuggler can impose a significant price premium. Profits derive from avoiding taxes or levies or restrictions on imported goods. For example, a smuggler might purchase a large quantity of cigarettes in a place with low taxes and smuggle them into a place with higher taxes, where they can be sold at a far higher margin. The following are the main focus of smuggled contraband.

Gas & Oil Smuggling

Gas & oil most profitable smuggling continues to be an issue in countries such as Nigeria, Iran and even Mexico. According to Iranian counter-smuggling authorities, 17% of daily fuel production equivalent to some 40mio liters were being smuggled out of the country every day in 2009. This is while most of the smuggling concerns gasoline and diesel fuel, whereas Iran imports both of these to the tune of 30 million liters every day. Smugglers are using underground pipelines to neighboring countries and oil tankers on the Shatt al-Arab waterway. Iran says its naval security forces have confiscated ten oil tankers smuggling 4,600 tons of Iranian fuel out of the Persian Gulf in 2008. As of 2012, smuggling to Pakistan and Afghanistan continues unabated because of price differentials with these countries. Now about one million liters of fuel is trafficked out of Iran every day.

Another example this time in the US when on 11 August 2009, the US Justice Department reported that US refineries were buying vast quantities of stolen oil from Mexican government pipelines. Criminals, especially drug gangs, tap remote pipelines and sometimes build their own pipelines to siphon off hundreds of millions of dollars worth of oil each year. The US Homeland Se-

curity Department is to return US\$2.4mio to Mexico's tax administration, the first batch of money seized during a joint investigation into smuggled oil.¹⁹

Cigarette Smuggling

Cigarette smuggling is a global problem, which continues to increase in spite of Governments' enforcement strategies. Cigarettes are of high value, highly taxed, readily portable and ideal commodities to be traded illegally. Cigarette smuggling appears to have been developed by organised crime groups as a global criminal business and generates huge profits for those involved.

In 2012 the FATF issued a report titled, "Illicit Tobacco Trade". The report details the affects that smuggling of tobacco has on governments, law enforcement, the tobacco industry, the health industry and others. Specifically, the implications that come from tobacco smuggling are: (1) Deprivation of tax revenues to governments. (2) Redirection of limited government resources to address tobacco smuggling. (3) A disproportionate effect and impact on health services. This is exacerbated by decreases in tax revenue and simultaneously fuels debate to increase taxes on tobacco which in turns stimulates the incentive to increase smuggling activities. (4) Legitimate brand holders struggle to compete in and against a black market created by tobacco smuggling.²¹

The chain of events that must occur for the successful smuggling of tobacco do not include money laundering until the very last step, selling the smuggled tobacco. At that point the illegal money must be laundered. Since organised criminal gangs have a heavy hand in tobacco smuggling it can be assumed that these gangs also have efficient ways and means of successfully laundering the profits of such an operation. See [Organised Crime](#).

Wildlife Smuggling & Poaching

Wildlife smuggling involves the illegal gathering, transportation, and distribution of animals and their derivatives, either internationally or domestically.²² It results from the demand for exotic species and the lucrative nature of the trade. The [CITES \(Convention on International Trade in Endangered Species of Wild Fauna and Flora, 1975\)](#) regulates the movement of endangered wildlife across political borders. Products demanded by the trade include exotic pets, food, traditional medicine, clothing, and jewellery made from animals' tusks, fins, skins, shells, horns, and internal organs.²³ In June of 2012, CITES reported that elephant poaching levels are the worst in a decade and ivory smuggling seizures are at their highest levels since 1989. Smuggled wildlife is an increasing global demand: it is estimated that the US, China, and the EU are the places with the highest demand. Interpol estimates that wildlife smuggling transactions generate between US\$10–20bio annually.

Alcohol Smuggling

Alcohol smuggling has some of the same characteristics in regards to its harms on society as a whole, but is not

as easy to physically smuggle as cigarettes. The smuggling of alcohol is usually done to avoid or circumvent taxation or prohibition laws within a particular jurisdiction. For example, certain Muslim countries, like Iran, forbid the drinking of alcohol therefore Iran has large criminal operations that are involved in the smuggling of alcohol across its borders.

The smuggling of alcohol deprives governments of tax revenues. This is especially true in the UK where authorities reported sales of illegal beer increased by 45% in 2009–2010. The smuggled alcohol was worth US\$1.2bio.²⁴ Smuggling operations also starve law enforcement resources that must be redirected to combat alcohol smuggling operations when the resources could be better used more serious crimes. The smuggling of alcohol also affects legitimate alcohol companies whose products are undercut by cheaper products that are smuggled instead of being purchased on legitimate markets that are legally taxed.

An example of Alcohol Smuggling from Canada to the US is the case of [Pasquantino](#).

Precious Metals & Stones Smuggling

Precious Metals & Stones smuggling remains a significant problem particularly in Africa, the proceeds of which have financed bloody civil wars. For more see [Precious Metals and Stones Dealers](#) later in Part 2, Sub-section 2 below.

Human Smuggling

For details see [Human Trafficking](#) above.

Arms Smuggling

For details see [Illicit Arms Trafficking](#) above.

Cash Smuggling

According to FATF's report in 2006 entitled "Trade-Based Money Laundering", the second of "three main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy" is "the physical movement of banknotes using methods such as cash couriers and bulk cash smuggling." In its paper, "Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments", FATF defines cash couriers as "natural persons who physically transport currency and BNI (bearer negotiable instruments) on their person or accompanying luggage from one jurisdiction to another." Bulk cash smuggling is defined as "the act of making a physical cross-border transportation of currency and BNI in large volumes where the currency/BNI is concealed in order to evade the reporting requirement, often using vehicles or containerized cargo or mail."²⁵

It is estimated that the [Mexican Drug Cartels](#) smuggle approximately US\$20–30bio a year, back from the US, using any of the 417 official border crossings between the US and Mexico, and the many unofficial crossing

points across the border. In 2011, US Immigration and Customs Enforcement reported only US\$150mio in seized cash and 428 arrests in bulk cash smuggling cases.

There are 417 official border crossings between the US and Mexico, and note I said "official" border crossings. One of the methods that the bulk cash smugglers will use is a form of smurfing or structuring where an individual carries approximately US\$5,000–10,000 on his person and crosses the border.

A typical bulk cash smuggling scenario, would look like the following: Money from the sale of drugs for example in New York City, would be taken to what is called a local stash house, or to a central counting location. That money arrives in the form of small dollar bills, usually fives, tens, 20s etc. These need to be refined and turned into larger dollar bills so as to reduce the mass size and make it easier to conceal and to transport. They are then vacuum packed into airtight plastic bags and surrounded with coffee grounds or pepper or other strong substances to thwart drug-sniffing dogs, and the packs are hidden in a vehicle, usually cars or trucks in some sort of hidden compartment. Vehicles are rotated as are drivers, so the same vehicles, drivers and plates are not identified. Further, they use advanced counter surveillance techniques, so they're surveying law enforcement too. They will also be at the border crossings on both sides, using high tech communications and surveillance, watching the border crossing to look to see what lane looks to be the best lane to go through and if there's anybody getting stopped.

Aside from vehicles, one of the methods that the bulk cash smugglers use is a form of smurfing or structuring where an individual carries approximately US\$5,000 to US\$10,000 personally across the border.

Once the cash arrives in Mexico much has traditionally been banked with Mexican financial institutions, including Money Services Businesses such as Casa De Cambios. Mexican Banks and Casa de Cambios would credit an account or wire the monies to a third account, oftentimes abroad, and then send these narco dollars (via armoured truck) back to their affiliates and/or accounts in the US or selling the dollars back to a US bank.

In order to address this problem the Mexican government has announced that it will limit individual bank account holders to deposits of no more than US\$4,000 a month, which should not affect the average Mexican household because the average Mexican household makes far less than US\$4,000 a month.

In response transshipments are being made avoiding direct approaches to financial institutions. According to FATF's 2008 "Terrorist Financing" typology report, "Counter-terrorist operations have shown that cash couriers have transferred funds to a number of countries

within the Middle East and South Asia. Direct flight routes are used for simple transfers; however, indirect routes using multiple cash couriers and changes in currencies take place within more sophisticated schemes."²⁶ Cash couriers are widely used in countries such as Africa and Middle East which have cash-based societies. (see [Money Services Business](#) in Part 2, including [Chop](#), [Fei ch'en](#), [Hawala](#), [Hundi](#) and others).

The FATF developed Special Recommendation IX in 2004 (now Recommendation 32) stating that countries should have measures in place to detect such transportation including a declaration system or other disclosure obligation. The legal authorities should stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering or that are falsely declared or disclosed. Sanctions should be available and measures adopted that enable the confiscation of such currency or instruments.

The higher denomination banknote allows for large sums of money to be smuggled cross-border in less weight and bulk to be carried over and thus avoiding being searched at the border. The high value banknotes are disproportionately used for money laundering such as the CAD1,000 and €500 notes. The Serious Organised Crime Agency claimed that 90% of all €500 notes sold in the UK are in the hands of organised crime. The €500 note is worth in the region of £430 depending on exchange rates (more than eight times the value of the Bank of England's largest publicly-circulated note, the £50 Note and has become the currency choice for gangs to hide their profits. Is it still in existence? It is also dripping with security measures as befits the world's second-highest denomination note (only the little-used 1,000 Swiss Franc has a higher value): watermarks, hologram strip, reflective glossy stripe, EURion constellation, matted surface, bar-codes, ultraviolet ink, perforations, raised printing, colour-changing ink and a serial number, all making it very difficult to counterfeit but still highly desirable to drug traffickers, money Launderers, and terrorists. The notes used to be nicknamed the 'bin Laden', because you knew they were out there, and you knew what they look like, but no one ever sees them. Of course that was before the US finally caught up with bin Laden in 2011.

The introduction of the €500 note in 2002 was a real benefit for the drug dealers as to transport the equivalent of US\$1mio required two suitcases but after the new notes were introduced, the same amount can fit into a backpack. The focus has switched from drugs going from Colombia to the US to drugs flooding Europe, where cocaine sells for roughly twice the amount as in America, and they can hide the money with much less difficulty. The drugs go in through Spain, often via West Africa, and then the euros come back out to the drug traffickers lords in Colombia, in Cali or Medellin or Bogota. Banking regulations in Colombia mean that any deposit over US\$10,000 is notified to the authorities and anyone trying to deposit large amounts

of €500 notes in a Bank would be sure to raise suspicion so instead they use the scores of casa de cambios many unregulated which have sprung up all across Latin America, particularly in Chile, Colombia, Ecuador, Peru and Venezuela. These will exchange foreign currency for local pesos, or courier the notes over to the US to be deposited in a legitimate bank. They then have the money wired back to the drug gang accounts in their home country. As an indication of their importance Colombia's financial regulator, believes 90% of the €500 notes currently in circulation worldwide (outside the EU) are being smuggled into Colombia.

A typical cash smuggling scenario looks like the following; the Euro's will be sent back via smurfs on planes from Spain, first arriving in Venezuela, Ecuador or Peru. Either they change it into pesos at a casa de cambio in those countries, or put it in a backpack to cross into Colombia along the long stretches of the border that are unmanned.

For other Cash Smuggling schemes and techniques and/or vulnerabilities see Hawala, Chop, Hindi etc in Part 1, Section 2, Sub-section 2, Money Services Businesses below and Part 1, Section 1, for Terrorism Finance above and see Part 2, Section 5, Criminals & Terrorists and Section 7, Criminal Cases.

One of the most important is used by Latin American Drug Trafficking Organisations, the BMPE.

Black Market Peso Exchange (BMPE)

Black Market Peso Exchange is a trade-based money laundering system used by Colombian drug cartels. It was discovered in the early 1990s. The Colombian peso brokers purchase illicit funds from criminals from other countries. They often deposit the money into their US bank accounts and sell cheques and wire transfers drawn on those accounts to legitimate business. The Colombian drug dealers export drugs to North America and Western Europe where they get paid in the foreign currency. The dealers convert this foreign currency into Colombian pesos with the help of a peso broker who exchanges the pesos he controls in Colombia for the funds the cartel holds in the foreign countries. The currency broker places these funds into the country's banking system and moves it around. The broker then advertises to Colombian importers that he has foreign funds available for the purchase of foreign products. Contacts of the broker purchase from manufacturers on behalf of the Colombian importers and the broker pays for the products with the drug money. The broker is paid in pesos by the Colombian importers refilling the broker's supply of peso currency funds.

The Black Market Peso Exchange is the largest known money laundering system in the Western Hemisphere, responsible for moving an estimated US\$5bio worth of

drug proceeds per year, from the US to Colombia. Other trade based methods for money laundering include manipulating trade documents to over or under paying for imports and exports and using criminal proceeds to buy gems and precious metals

Terrorism Finance

"Money is the lifeblood of terrorist operations. We're asking the world to stop payment." and "We will starve the terrorists of funding"

Former US President George W. Bush 2001¹

Harms

The major impact of terrorism is not the loss of life, the cost of responding to their activities or even the often times loss of hard won civil liberties, all of which are painful, but on the psychology of a society traumatised by fear and in part terrorised by the atrocities they read and hear about through the media. Whilst this fear is real, the reality remains that a citizen is much more likely to take his own life, be killed in a traffic accident or even drown in a swimming pool than be the victim of a terrorist attack. This is not to minimise the effect of fear and the natural and legitimate desires of societies to protect themselves and to react against deviant and aggressive behaviour. It is also the case that in part the fear is generated by concerns over terrorist's ability to gain access to and use weapons of mass destruction, creating the potential for harm on an almost unimaginable basis. Whilst the traditional view of terrorism was that terrorists would seek to limit casualties so as to make an impact but not to cause an excessive damaging response, the events of 9/11 changed that view. Though the traditional view may still hold for the majority of the major terrorist organisations, Al-Qaeda has clearly departed from that view and only the complacent would consider Al-Qaeda as either a spent force or unwilling if it had the means to use WMD. This is also why Rogue States engaged in developing WMD also cause greatest concern.

Statistics

Terrorist Groups designated by Leading Countries: Australia, Canada, EU, UK, US, India, Russia, China and Turkey include more than 150 groups, though almost none by all, as each country described and designates groups that represent threats to that country but also reflects differences in opinions and, of course, international politics. Paul Ashley in his book the "Complete Encyclopedia of Terrorist Organisations"² lists around 300 terror groups as being perhaps the most important but accepts there are even more that he does not mention. A few are no longer in existence, some have graduated to formal legal opposition, local or government parties, but many remain violent, outlawed and feared by those they oppose. Still most groups are not proscribed as terrorists outside of their borders. Within these 300, all shades of extremism are captured, including religious, nationalist and political,

covering the entire spectrum, from those exhibiting fundamentalist Christian, Jewish and Islamic tenets, minority and separatist groups and extreme right and left wing idealogues and combinations thereof.

Whilst both the US and UK (and EU) include many so called Islamic groups in their limited lists, differences even here exist between two countries with similar attitudes and responses to terrorism. For example, the US list includes, the Shining Path in Peru and the FARC in Colombia, close to home perhaps in South America, both of which are omitted from the UK and EU lists. The US list also includes Hamas and many Palestinian Groups including the Al Aqsa Martyrs Brigade and Lebanon's Hezbollah, whereas the UK and EU mentions only the military wings of both Hamas and Hezbollah and ignores many Palestinian groups like the Aqsa Martyrs Brigade. The UK list includes many Irish Terrorist groups beyond the Provisional IRA.

Whilst Islamic groups certainly appear prevalent in lists of groups designated beyond their immediate borders their significance (beyond Al-Qaeda) internationally is more in the fear they generate than in the true nature of their impact internationally. According to the US Dept of State who last published statistics on the number of known terror organisations by country, in 2004, rated Afghanistan with 13, Pakistan with 12, Lebanon with 10, India with 9, Ireland with 8, UK with 7, Iraq and Israel with 6, Philippines and Turkey with 6 each. According to MPT Terrorism Knowledge Base countries suffering the most fatalities from terrorist attacks (1968-2006) were; Iraq (11,760), US (3,227), India (1,556), Pakistan (1,555), Israel (1,454), Colombia (1,399), Russia (1,356), Lebanon (1,276), Algeria (983) and Afghanistan, (888).

When we think of countries most at risk of terrorist attacks, we usually think of Iraq, Pakistan or Afghanistan. Whilst these countries remain in the top 5 countries at risk, according to a 2011 report from Maplecroft, Somalia is now more at risk than any other country in the world and with the fledgling state of South Sudan also making the top five at number 5.³ The Top 4 countries are believed to sustain over 75% of world's fatalities from terrorism with terrorist attacks are on the increase globally. The 'extreme risk' category also includes: Yemen (6), Palestinian Occupied Territories (7), DR Congo (8), Central African Republic (9), Colombia (10), Algeria (11), Thailand (12), Philippines (13), Russia (14), Sudan (15), Iran (16), Burundi (17), India (18), Nigeria (19) and Israel (20)

Top 5 At Risk Countries for Terrorist Attacks		
1	Somalia	Extreme - 1,385 rating
2	Pakistan	Extreme - 2,163 rating
3	Iraq	Extreme - 3,456 rating
4	Afghanistan	Extreme - 3,423 rating
5	South Sudan	Extreme - 211 rating

Source: Maplecroft 2011

Looking at the year-on-year data, Maplecroft's research also reveals that the number of terrorist attacks rose by approximately 15% globally, with 11,954 incidents between April 2010 and March 2011, compared to 10,394 from April 2009 to 31 March 2010. However, there was a decrease in fatalities falling to 13,492 from 14,478. Significantly the research also reveals that the number of terrorist incidents in Afghanistan increased by over 50% over the same period, rising from 2,246 attacks in 2009/10 to 3,470 in 2010/11.⁴

According to the Global Terrorism Database (GTD),⁵ an open source event database that includes 82,000 domestic and international terrorist attacks since 1970. The GTD shows that Terrorist attacks reached their 20th century peak in 1992 (with over 5,100 attacks worldwide), but had substantially declined in the years leading up to the 9/11 attacks. In fact, total attacks in 2000 (1,351) were at about the same level as total attacks in 1977 (1,307) and worldwide terrorist attacks through the mid-1970s were relatively infrequent, with fewer than 1,000 incidents each year. From 1976 to 1979 the frequency of events nearly tripled. The number of terrorist attacks continued to increase until the 1992 peak, with smaller peaks in 1984, at almost 3,500 incidents, and 1989, with over 4,300 events. After the first major peak in 1992, the number of terrorist attacks declined until the end of the twentieth century, before rising steeply to a 10-year high of nearly 3,300 in 2007 – four years after the start of the Iraq war. Still, total attacks in 2007 were 36% lower than total attacks for the 1992 peak.

Fatal attacks also declined in the years prior to the 9/11 attacks. In fact, fatal attacks in 2000 (580) were considerably lower than they had been more than two decades earlier, in 1979 (832). In general, the number of fatal attacks clearly followed the pattern of total attacks. Fatal attacks rose above 1,000 per year for the first time in 1980. After hovering close to 1,000 attacks annually for most of the 1980s, they more than doubled between 1985 and 1992. Like total attacks, fatal attacks declined somewhat after 1992, bottoming out in 1998 with 426 attacks and then rising again to a global peak of more

than 2,100 fatal attacks in 2007. The peak in 2007 (2,111) was similar to the peak in 1992 (2,178).

In short, in the four years prior to 9/11 worldwide terrorist attacks and fatal attacks were at their lowest level in 20 years. However, both total and fatal attacks have increased considerably since then so that in 2007 total attacks were back to levels they had been at in the mid-1990s and fatal attacks were approaching the peak year of 1992.

Most frequently attacked Countries by Terrorists

1	Colombia	6767
2	Peru	6038
3	El Salvador	5330
4	India	4318
5	UK / NI	3762
6	Spain	3165
7	Iraq	3161
8	Turkey	2691
9	Sri Lanka	2611
10	Pakistan	2536
11	Philippines	2490
12	Chile	2287
13	Israel	2140
14	Guatemala	2023
15	Nicaragua	1986
16	South Africa	1921
17	Lebanon	1913
18	Algeria	1650
19	Italy	1487
20	US	1362

Sources: Global Terrorism Database since 1970

The US has long been perceived as being the target of an inordinate number if not a majority of terrorist attacks, though this is in fact not the case. Indeed Colombia is at the top with the most attacks and Iraq with the most fatalities. Latin America had the largest number of terrorist attacks of any region of the world throughout the 1980s and the first half of the 1990s. Four Middle Eastern or Persian Gulf countries are in the top 20 (Iraq, Turkey, Israel and Lebanon) and four are in South Asia or Southeast Asia (India, Pakistan, Sri Lanka, Philippines). Western Europe contains three countries in the top 20 (UK / Northern Ireland, Spain and Italy).

South Africa and Algeria are the sole countries from Africa in the top 20 most frequently targeted countries.

Most Fatalities by Country from Terrorist Attacks

1	Iraq	17,754
2	Sri Lanka	14,272
3	India	14,434
4	Colombia	13,009
5	Peru	12,496
6	El Salvador	12,496
7	Nicaragua	11,324
8	Algeria	8,545
9	Philippines	6,304
19	Pakistan	5,540
11	Guatemala	5,135
12	Turkey	4,674
13	Burundi	4,080
14	Afghanistan	3,764
15	US	3,394
16	Rwanda	3,200
17	Lebanon	3,093
18	Russia	3,057
19	Angola	2,861
20	UK / NI	2,842

Source: Global Terrorism Database since 1970

The direct international impact of Islamic terrorism on fatalities for example in the last 5 years has been around 5% of the total in North America and less than half a percent in Europe, with the EU only facing one Islamist terrorist attack in 2008. Separatist terrorism remains the terrorism area which affects the EU most. This includes Basque separatist terrorism in Spain and France, and Corsican terrorism in France. Past contacts between ETA and the FARC illustrate the fact that also separatist terrorist organisations seek co-operation partners outside the EU on the basis of common interests. In the UK, dissident Irish republican groups and other paramilitary groups may continue to engage in crime and violence. Nevertheless many of the most well publicized terrorist events carried out in recent memory have been carried out by so called Islamic Terrorists. Al-Qaeda attacks are often ones that are publicised and followed by the International media and where details about the funding of these attacks are available following detailed investigations. Whilst the following

are not exhaustive they are indicative and highlight the relatively small amount of funds required to carry out these significant attacks. These include; 9/11 in 2001 which was estimated to have cost around US\$400,000 -US\$500,000,⁶ the Bali Bombings in 2002 estimated at US\$20,000-US\$35,000, the Istanbul bombings less than US\$40,000, 1998 Africa US Embassy bombings less than US\$50,000, the first World Trade Centre attempted bombing US\$18,000, Madrid Train Bombings US\$60,000 and London underground and transport bombings US\$15,000. Whilst these amounts are not particularly large, denying access to funds will disrupt terrorist activities, in recruitment, in their day to day operations and in being able to carry out lethal activities. In the first few months after 9/11 the US announced that US\$112.2mio had been frozen worldwide which included significant funds of the Taliban regime already frozen since 1999. This increased by 2003 to US\$136mio and by 2005 US\$147mio, with at least US\$36mio frozen by US, US\$24mio by the Swiss, US\$11.9 by the UK, US\$5.5 by Saudi Arabia, and undisclosed amounts by the UAE, Pakistan and Turkey. The amounts frozen relating to the Taliban have since been returned to the Afghan government. Amounts frozen or interdicted for non-Al-Qaeda groups (including the Taliban) or beyond Hamas or Hezbollah remain minuscule.

Definition / Description

There is no single, universally accepted, definition of terrorism, though most agree that it involves the unlawful use of force and violence against persons or property to intimidate or coerce a government or the civilian population, to achieve political or social change.

Many attempts have been made but no final consensus has yet been reached. The Iranians in 1987 suggested, "Terrorism is an act carried out to achieve an inhuman and corrupt objective, and involving a threat to security of any kind, and violation of rights acknowledged by religion and mankind,"⁷ the US in 1989, "premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents,"⁸ the UN in 1992, simply, "Act of Terrorism equals Peacetime Equivalent of War Crime,"⁹ and in 2002 the EU, "given their nature or context, acts which may seriously damage a country or an international organisation where committed with the aim of seriously intimidating a population."¹⁰

The terms terrorism and terrorist are sometimes used to denote opposition to another and to justify this opposition. Existing regimes will often claim that separatists or insurgents are terrorists and now more than ever, with the label of terrorist being one which

should justly ensure all opposition. The phrase one man's terrorist is another man's freedom fighter is a well worn one but often apt. Take a look at the Assad regime's claims in Syria, that the opposition to dictatorial rule is by terrorists, which was a similar refrain from Colonel Gaddafi in Libya and President Ben Ali in Tunisia shortly before the opposition led successful strategies to throw these illegitimate rulers out. Whilst this difficulty exists in countries and against regimes that are plainly undemocratic, the challenge on defining a terrorist should be easier in countries enjoying representative democracy. In reality the term terrorism and terrorist is used by many but only gains real traction against those who challenge the order of the International Community at large. It also is worth noting that there can be a change in view over time, for example, in the 1850s, John Brown was a US abolitionist who advocated and practiced armed opposition to slavery. Brown led a series of attacks between 1856 and 1859, the most famous in 1859 against the armoury at Harper's Ferry. Local forces soon recaptured the fort and Brown was tried and executed for treason. A biographer of Brown has written that his purpose was "to force the nation into a new political pattern by creating terror." More recently, Nelson Mandela was for a time by some considered a terrorist and now greatly respected as one of the world's greatest statesmen, Osama bin Laden, considered a freedom fighter and liberator when fighting the Soviets in Afghanistan and a terrorist once he turned on the West and Yasser Arafat, a Terrorist as head of the PLO, earlier the Al-Fatah faction, then a Statesman after signing the Oslo Peace Agreement with the Israelis and then later as a de facto terrorist once more, once it was clear Oslo was not being implemented. Terrorist financing refers to financing of terrorist groups and their activities.

State Sponsorship of Terrorism

Whilst in some States, its institutions such as the Army, Police or Security Agencies or their proxy militias or thugs may effectively terrorize opposition elements within the State, however, its perpetrators are rarely identified as terrorists. Such actions are criticized but largely disputed and seen by many as an internal matter for the State and its citizens and not for third parties to decide. When, however, States get involved directly in terror operations beyond their borders or where they provide material support to a terror organization then a State may be described as a State sponsor of Terror. When terror is officially sanctioned by a State, government personnel will organize and arrange and carry out the terrorist operation, although such official sanction will rarely be acknowledged. This was the case of Libya, which authorized and carried out the downing of a Pan Am transatlantic flight in 1998.

over Lockerbie in Scotland. Libya also authorised and arranged for the attempted assassination of the Saudi Crown Prince Abdullah in 2003. For details see the case of Abdulrahman Alamoudi in Part 2, Section 7. State sponsorship of terrorism or "state supported" terrorism, is somewhat different and involves a State providing supplies, training, and other forms of support to non-state terrorist organizations, for example a safe haven, false documentation, financing and weapons or the extension of diplomatic services to the terrorists. Examples of state sponsorship is the Syrian government's support of Hamas in Palestine and Hezbollah in Lebanon. Syrian resources and protection enable the huge training establishments in the Bekaa Valley. Another example was the Taliban in Afghanistan who provided a safe haven to Al-Qaeda. On a smaller, more discreet scale, the East German Stasi provided support and safe-haven to members of the Red Army Faction (RAF or Baader Meinhof Gang) and neo-fascist groups that operated in West Germany. Wanted members of the RAF were found resident in East Germany after the fall of the Berlin Wall in 1989.

The Convention on Offences and Certain Other Acts Committed on Board Aircraft, 1963,¹¹ (commonly known as the "Tokyo Convention") was the first of its kind to recognize certain powers of the aircraft commander to restrain anyone believed to pose a safety risk to other passengers. It was followed in 1970, by the Convention for the Suppression of Unlawful Seizure of Aircraft and in 1971,¹² by the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation.¹³ Supplementary protocol was added to the 1971 convention detailed in the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (1988).¹⁴ In 2005, Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation¹⁵ was adopted to ensure that appropriate action is taken against persons committing unlawful acts against ships. Also in 2005, Protocol to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf¹⁶ was produced in order to reflect amendments to the 1988 protocol of the same name. In 1997, the International Convention for the Suppression of Terrorist Bombings¹⁷ was designed at the UN's Terrorist Bombings Convention. Further to this, in 1999, the International Convention for the Suppression of the Financing of Terrorism¹⁸ was adopted.

Historical Background / Context

Terrorism is hardly a new phenomenon, and has affected the established order throughout time. An early example in the 1st century AD were the Jewish Zealots in Judea (today's Israel), who rebelled against Roman rule, attacking both Jewish "collaborators," including temple priests, and other wealthy elites. The Zealots hid

short daggers under their cloaks, mingled with crowds at large festivals and murdered their victims, then disappearing into the panicked crowds. Their motive was an uncompromising belief that they could not remain faithful to the dictates of Judaism while living as Roman subjects. Eventually, the Zealot revolt became open and the groups were finally besieged and committed mass suicide at the fortification of Masada. The Assassins were the next group to show recognizable characteristics of terrorism, as we know it today. A breakaway faction of Shia Islam called the Nizari Ismailis adopted the tactic of assassination of enemy leaders because the cult's limited manpower prevented open combat. Their leader, Hassan-I Sabbah, based the cult in the mountains of Northern Iran. Their tactic of sending a lone assassin to successfully kill a key enemy leader at the certain sacrifice of his own life (the killers waited next to their victims to be killed or captured) inspired fearful awe in their enemies. Both the Zealots and the Assassins can be seen as forerunners of modern terrorists, with similar motivation, organisation, targeting, and goals. Secondly, although both were ultimate failures, the fact that they are remembered hundreds of years later, demonstrates the deep psychological impact they caused.

Other examples could include the Gunpowder Plot, in the 17th Century, an attempt to destroy the English Parliament in 1605 and in the 18th Century, the Boston Tea Party which preceded the American Revolution. The French Revolution provided the first uses of the words "Terrorist" and "Terrorism", however conversely the use of the word "terrorism" began in 1795 in reference to the "Reign of Terror," initiated by the government, who became known as the "Terrorists". The French Revolution provided an example to future states in how to oppress their populations. It also inspired a revolutionary reaction which started by opponents who employed terrorist tactics such as assassination and intimidation. The Parisian mobs also played a critical role at key points before, during, and after the Revolution, killing prominent officials and aristocrats in gruesome spectacles. The tactics of the French State were not new and would be followed by the new Russian State in 1918 as the Bolsheviks sought to concentrate power and authority and later by Nazi Germany's Gestapo in the 1930s and 40s. Incidentally, it was the Nazi occupiers of Europe during the Second World War who characterized the work of the French, Czech, Polish, and other resistance movements, supplied and fomented by Britain's Special Operations Executive, as "terrorism."

After the Second World War, a series of anticolonial movements for example the Viet Minh against French rule in Vietnam, used the wartime tactics of resistance to attack the French with classic terror tactics, in order to undermine French rule and morale. Similar tactics

were used against the British in Palestine by Israeli groups freedom fighters / terrorists like the future prime ministers Menachem Begin and Yitzhak Shamir leaders in the The Irgun and Stern Gangs who blew up civilians in hotels, assassinated British troops, and ambushed British patrols, in order to achieve the founding of the State of Israel. Following on, the National Liberation Front of Algeria fought French rule with a ruthless terror campaign. The French fought back ferociously and whilst the Battle of Algiers was a military victory, it was a political defeat, leading to the collapse of the French government and returning to power wartime hero Charles de Gaulle, who eventually launched negotiations that led to Algerian independence in 1962.

Airline Attacks

The age of modern terrorism might be said to have begun in 1967-8, with the Arab-Israeli Six Day War of 1967 and the worldwide student movements of 1968. The devastating Arab defeat and the Israeli occupation of the West Bank and Gaza Strip inspired the Palestine Liberation Organisation, too weak to fight an orthodox struggle, to adopt terrorist tactics. Other pro-Palestine groups imposed their demands on a global audience by hijacking airliners and kidnapping Israeli athletes at the 1972 Olympic Games in Munich. Young militants in Europe, Japan, and the US turned to similar tactics for different reasons. In Northern Ireland, a Protestant backlash against the campaigns of the Roman Catholic civil rights movement revived the Irish Republican Army. West Germany's Red Army Faction, Japan's Red Army, and Italy's Red Brigades made common cause with the PLO. They used their training camps and cooperated with each other conducting operations, such as kidnappings and killings against as they saw it fascist capitalism that had taken over their countries.

In Latin America, Castro's Cuba showed many a communist alternative attractive to some and repugnant to others. The left-right battles that waged led to the rise of the Shining Path, Tupac Amaru in Peru, the Movement of the Revolutionary Left in Chile and the FARC and ELN in Colombia amongst many others. Increasing prosperity and a move to greater democracy has diminished many groups though some remain.

With the ending of Soviet support with the end of the cold war, and increased international co-operation, most of these terrorist groups have been defeated or marginalized. Those that survived, the PLO and the IRA, ETA, and the FARC perhaps sustained by a degree of popular legitimacy that stemmed from their origins as national liberation movements have all sought and entered into dialogue with differing levels of success.

Today the rise of Al-Qaeda and other Islamic groups, presents new challenges but also familiar ones. History predicts that they will either be defeated or exhausted or seek to compromise and enter a dialogue and move away from terror tactics. History also predicts the continued existence of States that in one way or another inflict fear and terrorize their citizens. The age of modern terrorism might be said to have begun in 1968 when the Popular Front for the Liberation of Palestine (PFLP) hijacked an El Al airliner en route from Tel Aviv to Rome. While hijackings of airliners had occurred before and already in 1963 The Tokyo Convention (see above) had already been passed, this was the first time that the nationality of the carrier (Israeli) and its symbolic value was a specific operational aim. Also a first was the deliberate use of the passengers as hostages for demands made publicly against the Israeli government. The combination of these unique events, added to the international scope of the operation, gained significant media attention. The founder of PFLP, Dr. George Habash observed that the level of coverage was tremendously greater than battles with Israeli soldiers in their previous area of operations. "At least the world is talking about us now."

In response The 1970 Convention for the Suppression of Unlawful Seizure of Aircraft was passed followed in 1971 by the Convention for the Suppression of Unlawful Acts against the safety of Civil Aviation. Despite International action the internationalisation of terrorism and the cooperation between extremist organisations in conducting terrorist operations intensified. Cooperative training between Palestinian groups and European radicals started as early as 1970, and joint operations between the PFLP and the Japanese Red Army (JRA) began in 1974. Since then international terrorist cooperation in training, operations, and support has continued to grow, and continues to this day. Motives range from the ideological, such as the 1980s alliance of the Western European Marxist-oriented groups, to financial, as when the IRA exported its expertise in bomb making as far afield as Colombia. Whilst flying remains one of the safest forms of travel, incidents when they occur are more likely to result in fatalities. The first fatal aviation accident occurred in 1908, when Orville Wright crashed his Wright Model A aircraft during testing killing his passenger. It wasn't until 1933 that the first 2 Aeroplanes were destroyed intentionally first by fire and then by a bomb and is thought to be the first proven acts of air terror in the history of commercial aviation. Passenger airliners as well as cargo aircraft have been the subject of plots or attacks ever since.

Many early bombings though were suicides or schemes

for insurance money, but in the latter part of the 20th century, political and religious militant terrorism became the dominant motive for attacking large jets, either by hijacking, to publicize a cause or to make demands or by bombing to cause mass casualties. Whilst the political and religious motives are varied, many of the worst incidents, involve so called Islamic or Middle East Terrorists, from Pakistani based groups targeting India and supporting secession from India of Kashmir and Jammu provinces, Palestinian Groups fighting for their State, State sponsored terror from Libya, Chechens for Independence and Al-Qaeda for an Islamic Caliphate.

Whilst dynamite was first used, plastic explosive is the preferred form of bomb as it is both harder to detect and has greater explosive power. Whilst the most common form of terrorist attack was carried out by smuggling explosives into baggage, detonating the bomb once the Plane is in the air usually by timers, more recently with Al-Qaeda representing the most active threat the modus operandi has changed. Al-Qaeda have attempted numerous new ways of bringing down airplanes, including using suicide bombers to either directly crash the Planes or to explode bombs concealed on board or chemicals carried which when mixed can produce an explosion with devastating affects. Most recently Al-Qaeda have targeted cargo planes with bombs

The deadliest aviation-related disaster, considering fatalities on both the aircraft and the ground, was the attack on America on 9/11/2001, killing almost 3,000 people. The deadliest pure Aircraft disasters were not terrorist events. The first occurred in Tenerife when two Boeing 747 aircraft collided when a KLM Boeing 747 attempted take-off without clearance, and collided with a taxiing Pan Am 747 killing 583 people. The second was the crash of Japan Airlines Flight 123 in 1985 which resulted in the highest number of fatalities for a single aircraft. The Boeing 747 aircraft suffered an explosive decompression from an incorrect repair resulting in the death of 520 on board. The first recorded aircraft hijack took place in 1931, in Peru, when a pilot was approached on the ground by armed revolutionaries. Hijackings increased between 1948 and 1957, to 15 and climbed to 58 between 1958 and 1967. A shocking 38 deaths from hijackings occurred in 1968 followed by 82 in 1969, the largest number in a single year in the history of civil aviation. During the period between 1968 and 1977, there were 414 hijackings and between 1988 and 1997, there were 180 hijackings, the number dropping to 98 between 1998 and 2007. Since 2001 to the present day the numbers have fallen considerably to only 43 incidents.

World's Worst Airline attacks by Terrorists (causing 100 or more fatalities)

Deaths	Details
100	1973 - Aeroflot TU-104 exploded over Siberia after hijackers demands not met
110	1989 - Avianca Flight 203 exploded in Colombia, Pablo Escobar responsible
100	1977 - A hijacked Malaysian Boeing 737 airliner downed
112	2002 - China Northern Flight 6136 crashed in China after passenger suicide insurance attack
106	1993 - Transair Georgian Airlines TU - 154B downed by a missile in Georgia
112	1983 - Gulf Air 771, Boeing 737 downed from Pakistan by Abu Nidal Organisation
115	1987 - Korean Air Flight 858 downed by North Koreans
127	1996 - Ethiopian Boeing 767 crashed following hijacking by Ethiopians
132	1990 - Chinese Boeing 737 hijacked & crashed in China
171	1989 - French UTA Flight 772 DC - 10 destroyed over Niger by Libyans
217	1999 - Egypt Air Boeing 767 crashed off Massachusetts after pilot intentionally downed it
259	1988 - Pan Am Flight 103 downed over Lockerbie, Scotland by Libyans
331	1985 - Air India Flight 182 from Montreal downed by extremist Sikhs
2997	2001 - Attack on America on 9/11 by <u>Al-Qaeda</u>

Source: Author (See Part 2, Section 6 below)

As far as hijackings are concerned perhaps the most well known occurred in 1976 when Air France, with 139 passengers on board, was hijacked by Palestinian hijackers. A daring raid by Israeli special forces who landed at Entebbe Airport, Uganda, led to the rescue of almost all Israeli hostages and the killing all Palestinian hijackers (Popular Front for the Liberation of Palestine). However three passengers and one commando were killed. Whilst there are more than 85 cases related to airline attacks, with more than 50 of them resulting in deaths 34 of these are perhaps the most shocking mass casualty events and of greatest importance, indicating new threats and or targets or methods. For a summary of 34 of these attacks targeted at Airlines see Part 2, Section 6 below. Of these 34 there are 14 cases resulting

in 100 or more fatalities. Whilst the last decade has proven to be one where fatalities have been one of the lowest on record, this is due more to foiled and failed attempts, rather than any reduction in threat levels. Whilst Airline attacks have been a preferred method of attack, bombings and shootings are also common, both in the form of mass casualty events and of assassinations, the largest act of international terrorism occurred on September 11, 2001 in a set of co-ordinated attacks on the US where Islamic terrorists hijacked civilian airliners and used them to attack the World Trade Centre towers in New York City and the Pentagon in Washington, DC and attempted to destroy the US Congress building or the White House. In this way the terrorists had wanted to use Airlines as bombs and to cause both mass casualty and assassination at the same time. For details about this attack and more than 100 other major terror attacks see Part 2, Section 6.

Major Fatalities / Terrorist Attacks

202	2002 - Bali Bombings in Indonesia by <u>Jemaah Islamiyah</u>
233	1987 - Bus attacks in Sri Lanka by <u>Tamil Tigers</u>
300	1990 - Attack in mosques in Sri Lanka by <u>Tamil Tigers</u>
301	1983 - Truck bombings of US Marine & French barracks, Beirut by <u>Hezbollah</u>
301	1999 - Bombings of apartment buildings in Moscow Russia by <u>Chechen Terrorists</u> over 12 days
303	1998 - Truck bombings of US embassies in Nairobi, Kenya & Dar es Salaam, Tanzania by <u>Egyptian Islamic Group & Al-Qaeda</u>
317	1993 - 15 bombings in Bombay, India by <u>D-Company</u>
339	2004 - School Hostage Crisis, Beslan Russia by <u>Chechen Terrorists</u>
477	1978 - Cinema Rex Arson Abadan, Iran by <u>Iranian Revolutionaries</u>
2997	2001 - Attack on America on 9/11 by <u>Al-Qaeda</u>

Source: Author (see Part 2, Section 6 below)

Money Laundering

Terrorist Groups tend to flourish where they can find either a safe haven or where there is sufficient instability or where strong government control is missing. Safe havens include ungoverned, under-governed, or ill-governed physical areas where terrorists are able to organise, plan, raise funds, communicate, recruit,

train, transit, and operate in relative security because of inadequate governance capacity, political will, or both. Whilst Al-Qaeda and Al-Qaeda affiliates are the most well known there are many others that deserve attention and can be found in most regions of the world. What follows is a short summary of the most important. Individual Profiles of many of the terrorist groups can be found in Part 2, Section 5 below.

Africa

In Africa, Somalia. With its long unguarded coastline, porous borders, continued political instability, and proximity to the Arabian Peninsula, provides opportunities for terrorists and is considered a major safe haven, particularly for Al-Shabaab. Sudan remains a US designated State Sponsor of Terrorism since 1993, with elements of several terrorist groups including Al-Qaeda (AQ)-inspired terrorist groups remaining in Sudan, links to Palestinian groups and to Iran. South Sudan attained independence on July 9, 2011, becoming the world's newest country following a long struggle by the Sudan People's Liberation Army, and like its neighbours Uganda, the Central African Republic and the Democratic Republic of Congo (DRC) faces threats from The Lord's Resistance Army (LRA). Earlier similar struggles to that of the SPLA were undertaken by the National Union for the Total Independence of Angola (UNITA) and by the Mozambique National Resistance Movement (RENAMO) with both being effectively defeated. In the DRC which is a vast country bordered by nine neighbours, the Government continues to lack complete control over some large swathes of its territory, especially in the East in and around the Rwandan border where various groups operate, including the Rwandan Patriotic Army (Tutsi) and the Army for the Army for the Liberation of Rwanda (Hutu). In North Africa, in the Maghreb and Sahel regions, the primary terrorist threat is from Al-Qaeda in the Islamic Maghreb (AQIM), particularly until very recently operating from safe havens in Northern Mali and moving to other areas in the Maghreb and Sahel, such as Libya, Niger, and Mauritania, and also from Ansar Dine, a militant Tuareg group in Mali. Following the overthrow and killing of Libyan Leader Muammar Gaddafi in October 2011, an interim national government assumed power in Libya, though there remains a great deal of instability with rival armed groups maintaining control of local areas. It was rumoured that Al-Qaeda leader Zawahiri dispatched AQ fighters to eastern Libya and they remain operational, and that former terror group the Libyan Islamic Fighting Group, had reformed into a success organisation and joined the new coalition administrations. Elsewhere in the region the Armed Islamic Group in Algeria; the Moroccan Islamic

Combatant Group and the Tunisian Combatant Group are active. In West Africa, in Africa's most populous state, Nigeria, the extremist Islamic group, Boko Haram continues to create havoc across the north of the country and in the capital, Abuja, whilst the Movement for the Emancipation of the Niger Delta (MEND) does the same in the Niger Delta.

Middle East

Iraq was until the demise of Saddam Hussein a US designated State sponsor of terror. Whilst the successor governments and coalition forces have faced strong resistance from Sunni insurgency groups, they also faced attacks from Al-Qaeda in Iraq. As such Iraq was considered until recently a safe haven for some terrorist actors though improvements by the government and security forces and the inability to win support from the local Sunni community in Iraq has marginalized Al-Qaeda in the land of the two rivers or otherwise known as Al-Qaeda in Iraq (AQI). Also of note are Abdullah Azzam Shaheed Brigades, Ansar al-Islam, Jamaat Ansar al-Sunna and Khata'ib Hezbollah. Elsewhere in the Middle East, for example in the Lebanon, Hezbollah militias control access to parts of the Country as the Lebanese government does not exercise complete control over all regions. The areas outside the control of the government, some parts of Beirut, much of the South, near its borders with Syria and Israel are controlled by Hezbollah. Palestinian refugee camps are also used as safe havens by Palestinian terrorists and armed groups and are used to house weapons and shelter criminals and terrorists. Gaza more so but also including the West Bank are also safe havens for Palestinian terrorists. Also of note are Amal, Jund al-Sham and Asbat al-Ansar. In the Gulf region, where Saudi Arabia dominates, the government is fighting Al-Qaeda in the Arabian Peninsula and has largely been successful, though the southern province of Jazan adjacent to the Yemen is still an area where AQAP operates and has its base. Yemen's lack of a governmental presence in much of the country and its porous borders were exacerbated in 2011 by political instability, allowing Al-Qaeda in the Arabian Peninsula (AQAP) to retain existing safe havens in Yemen and establish new ones. In a tactical change, AQAP captured territory near Aden, in spring 2011.

Designated as a US State Sponsor of Terrorism in 1984, Iran remains an active state sponsor of terrorism increasing its terrorist-related activity, likely in an effort to exploit the uncertain political conditions resulting from the Arab Spring, as well as in response to perceived increasing external pressure on Tehran. Iran also continued to provide financial, material, and logistical support for terrorist and militant groups throughout the Middle East and Central Asia. Iran provides weapons

and training to assist the Asad regime in the current Syrian Civil War as well as providing weapons, training, and funding to Hamas and other Palestinian terrorist groups, including the Palestine Islamic Jihad and the Popular Front for the Liberation of Palestine-General Command. Since the end of the 2006 Israeli-Hezbollah conflict, Iran has assisted in rearming Hezbollah. Iran has provided hundreds of millions of dollars in support of Hezbollah in Lebanon and has trained thousands of Hezbollah fighters at camps in Iran. Whilst it is believed that Iran has detained senior AQ members it refuses to publicly identify them or take any public action against them. It is thought to allow AQ members to operate a corridor through Iranian territory, enabling AQ to carry funds and move facilitators and operatives to South Asia and elsewhere. In Iran itself the Mujahideen-e Khalq and Jundallah are threats and in Saudi Arabia and Yemen, the threat is from Al-Qaeda in the Arabian Peninsula as well as from an off-shoot, Ansar al-Sharia. Designated in 1979 as a State Sponsor of Terrorism, Syria continues its political support to a variety of terrorist groups affecting the stability of the region and beyond, even amid significant internal unrest. Syria provided political and weapons support to Hezbollah in Lebanon and continued to allow Iran to resupply the terrorist organisation with weapons. The external leadership of Hamas, the Palestine Islamic Jihad (PIJ), the Popular Front for the Liberation of Palestine (PLFP), and the Popular Front for the Liberation of Palestine-General Command (PFLP-GC), among others, were based in Damascus and operated within Syria's borders though Hamas began leaving the country in late 2011 over disagreements regarding Syria's use of violence against protestors. Statements supporting terrorist groups like Hamas and Hezbollah consistently permeated government speeches and press statements. The Syrian Baathist regime provides Iraqi exiled individuals safe haven in Syria, including Iraqi Baathists, with some of them calling for violence against the Iraqi government, Iraqi civilian targets, and American and coalition forces within Iraq. Syria also continues its strong partnership with fellow US state sponsor of terrorism, Iran. Since the outbreak of the Syrian Civil War groups have emerged to fight government forces who the Syrians call terrorists, including the Syrian Islamic Front; the Syrian Islamic Liberation Front; the Al-Nusra Front or Jabhat al Nusra and the Islamic State of Iraq and Syria, the latter believed to be close to or an off-shoot of or successor to Al-Qaeda in Iraq.

In Egypt, Islamic Jihad groups, for example, Egyptian Islamic Jihad and Gama'a al-Islamiyya, were aggressively targeted by the Mubarak government, with EIG's leader Ayman Zawahiri merging his group into bin Laden's Al-Qaeda and since his death succeeding him

as the leader of AQ. Gama'a al-Islamiyya (IG), was Egypt's largest militant group, originally formed by the coming together of militant student cells following the renunciation of violence by the Muslim Brotherhood, whose leader Mohammed Marsi became Egypt's President following democratic elections after the ouster of Mubarak, before being ejected again recently.

The Israel/Palestine conflict continues despite much of the leadership of the Palestine Liberation Organisation including Fatah, renouncing violence and signing up to peace treaties. Still parts of the West Bank and Gaza Strip are home to terrorist groups, in particular some groups that have splintered from the PLO such as, the Aqsa Martyrs Brigade, Tamzin Fatah, Palestinian Islamic Jihad, Popular Front for the Liberation of Palestine and also the Democratic Front for the Liberation of Palestine; the Palestine Liberation Front; the Army of Islam and to Hamas which originated as the Palestinian branch of the Muslim Brotherhood, founded in Egypt. The region was also home to legendary and notorious groups including Black September and the Abu Nidal Organisation as well as Jewish groups the Irgun and more recently Kahane Chai. Whilst sometimes considered part of Europe and at other times part of Asia, Turkey straddles the two and can also be considered part of the Middle East with its southern borders neighboring Syria and Lebanon, and its Eastern border neighboring Iraq. Separatist ambitions have long been held by the Kurds who live in Eastern Turkey and Northern Iraq, though both the Turkish government and the Iraqi governments have long since fought to prevent the establishment of "Kurdistan." The Kurdistan Workers Party (PKK) is the main terrorist group continuing the struggle for the establishment of a State for Kurds with others such as the Kurdistan Freedom Falcons and the Revolutionary People's Liberation Party-Front also included.

Asia

In South East Asia, the numerous islands in vicinity of the Sulawesi Sea and the Sulu Archipelago and around Mindanao in the Southern Philippines, Indonesia and in Eastern Malaysia make it a difficult region for authorities to monitor, and a range of licit and illicit activities occur there which pose additional challenges to countering the terrorist threat in the region. Terrorist organisations such as Jemaah Islamiya and the Abu Sayyaf Group constitute the primary terrorist presence although the New People's Army the Moro Islamic Liberation Front, the Free Papua Movement and Jemah Anshorut Tauhid are also present too. In Southern Asia, Afghanistan and Pakistan remain the two principal countries of concern, with the Taliban, the Hezb-e-Islami Gulbuddin, Al-Qaeda (AQ), the

Pakistan Taliban, Lashkar I Jhangvi, the Islamic Jihad Union Sipah-e-Sahaba, Jamiat-e-Islami, Tehreek-e-Nafaz-e-Shariat-e-Mohammadi and other groups who continue to use these territories to plot and launch attacks within the region and beyond. Portions of Pakistan's Federally Administered Tribal Areas (FATA), Khyber Pakhtunkhwa (KPK), and Baluchistan, in particular remain a safe haven for terrorist groups seeking to conduct domestic, regional, and global attacks. Given the inability of Pakistan's security agencies to fully control portions of its own territory, the Haqani Network and the Quetta Shura exploit the country to plan and direct operations. As far as Kashmir and Jammu are concerned this remains a hot spot and groups like Lashkar-e-Tayyiba continue to operate behind and across the Line of Control (the border along Jammu and Kashmir) between Pakistan and India. Other groups include Jaishe-Mohammed, Harkat-ul-Jihad-al-Islami, Harakat-ul-Mujahideen, Al-Umar Mujahideen, Dukhtaran-e-Millat, Hizb ul Mujahideen and the Balochistan Liberation Army. Whilst historically and until recently the terrorism from Pakistan, and the Civil War in Sri Lanka have been the greatest terrorist threats to India, according to Prime Minister Singh it is Maoist/Naxalite violence in other parts of the country which he calls "India's greatest internal security threat," coming from groups such as the Communist Party of India-Maoist. These groups are allied with The Communist Party of Nepal-Maoist and the Akhil Bharat Nepali Ekta Samaj that operates over the border in Nepal each with the goal of establishing communism and replacing the existing regimes. Sikh Terrorism is also a problem in India with Indian Sikh groups determined to carve out an independent Sikh state called Khalistan (Land of the Pure) from Indian territory. Many of these groups operate under umbrella organisations, the most significant of which is the Second Panthic Committee. Other active Sikh groups include Babbar Khalsa Int, Azad Khalistan Babbar Khalsa Force, Khalistan Liberation Front and Khalistan Zindabad/Commando Force. In Sri Lanka, the once mighty Tamil Tigers operated out of the North of the Island, particularly in the Jaffna Peninsula until their recent defeat by Government forces and in part financed by the World Tamil Movement of Canada and similar organisations elsewhere. Also active were the Tamil Nadu Liberation Army and the Tamil Rehabilitation Organisation both operating in Tamil Nadu in India. In Bangladesh, Islamist fundamentalist groups such as Jamaat-ul-Mujahideen and Harakat ul-Jihad-i-Islami are also active. India's so-called "Seven Sisters" region of small north eastern states has many active secessionist groups. The Kanglei Yawol Kanna Lup, the People's Liberation Front and the Revolutionary People's Front, the United National Liberation Front and the People's

Revolutionary Party of Kangleipak are all "mete" groups fighting for an independent state of Manipur. A number of groups are also active in Garoland including the Achik National Volunteer Council (ANVC), the Garo National Liberation Army, and the Hynniewtrep National Liberation Council (HNLC). Other groups active in Assam, Bodoland and Tripura respectively include the United Liberation Front of Assam, the National Democratic Front of Bodoland and the National Liberation Front of Tripura.

In China, terrorism is focussed on incidents of violence committed in Xinjiang province by separatist groups. Xinjiang, literally "new frontier," is a provincial-level autonomous region situated in the northwest of China. Attacks have increased by members of the largely Muslim Uyghur ethnic group, who identify more closely with the cultures of Central Asia and still resist attempts at assimilation with Han Chinese culture. Organisations identified by the Chinese government as having involvement in violent attacks include the East Turkistan Islamic Movement (ETIM), East Turkistan Liberation Organisation (ETLO), the World Uyghur Youth Congress and the Eastern Turkistan Information Centre. Members of these groups are believed to have received training in Afghanistan and Pakistan. This North West Region of China borders the Central Asian Republics, (CAR States), where the threat from Islamic groups particularly in Tajikistan and Uzbekistan is increasing. Tajikistan is unable to control the 900 mile Tajik-Afghan border, which is where many of the groups are trained and are based. The Islamic Movement of Uzbekistan (IMU) remains a threat, though is still mainly fighting in Afghanistan along with the Taliban. It is feared that many of the fighters in Afghanistan are closely linked to the IMU and will eventually turn their attention from Kabul to Tajikistan. The main terrorist threats in the region come therefore from the Islamic Movement of Uzbekistan, and its offshoots or affiliates Hizb ut-Tahrir al-Islami, Hizb-an-Nusra; Akromiya; Jama'at al-Jihad al-Islami also known as the Jamaat of Central Asian Mujahideen (JCAM), and Islamic Jihad Group (IJG), all of whom are seen as Islamic terrorist organisations affiliated with Al-Qaeda that operates in the Central Asian Region. Other groups relevant also include, the Kurdistan Workers Party, Lashkar-e-Toiba, Aum Shinrikyo and the East Turkestan Liberation Organisation, as each are banned in one or more of the CAR states.

Americas

In Central America, terrorist activity has subsided following the resolution of civil wars in past decades where, particularly El Salvador and Nicaragua, were hardest hit with groups such as the People's Liberation

Forces and Farabundo Marti National Liberation Front in El Salvador then active and the Nicaraguan Democratic Force also known as the "Contras" also then active in Nicaragua. Elsewhere in South America, similar groups operated during past trouble, for examples, in Argentina with the People's Revolutionary Army and the Anti-Communist Alliance, in Uruguay with the Tupamoros, in Bolivia with the National Liberation Army, in Chile with the Movement of the Revolutionary Left (MIR) and the Manuel Rodriguez Patriotic Front (FPMR). In Colombia which borders with Venezuela, Ecuador, Peru, Panama, and Brazil, rough terrain and dense forest cover which coupled with low population densities and historically weak government presence, have often allowed for potential safe havens for insurgent and terrorist groups, particularly the Revolutionary Armed Forces of Colombia (FARC) and the National Liberation Army (ELN) and before them the April 19th Movement and in response the United Self-Defence Forces of Colombia (AUC) and the Popular Revolutionary Anti-Terrorist Army of Colombia (ERPAC) including successor organisations such as the Black Eagles. The Tri-Border Area (Argentina, Brazil, and Paraguay), is also an area of concern. Whilst no credible information has showed that Hezbollah, Hamas or other Islamist extremist groups used the Tri-Border Area for terrorist training or other operational activity, there are concerns that these groups used the region to raise funds from local supporters. The Argentine, Brazilian, and Paraguayan governments have long been concerned with arms and drugs smuggling, document fraud, money laundering, trafficking in persons, and the manufacture and movement of contraband goods through the Tri-Border Area. Peru's primary counterterrorism concern remains Sendero Luminoso (or Shining Path). Although Peru eliminated the Tupac Amaru Revolutionary Movement, and almost eliminated SL in the 1990s, SL remains in tact and involved in and funded through narcotics trafficking is still a threat. Venezuela remains a concern not so much for the existence of the Bolivarian Liberation Forces largely inactive now but because of its close ties to US states sponsors of terror, Iran and Syria as well as North Korea and Cuba. Cuba in the Caribbean has been designated by the US as a State Sponsor of Terror since 1982. Current and former members of Basque Fatherland and Liberty (ETA) continue to reside in Cuba and the Cuban government is thought to provide medical care and political assistance to FARC in Colombia. The Cuban government also continues to permit fugitives wanted in the US to reside in Cuba and also provides some support for these individuals.

Europe

The major terror threat on the European continent comes from Al-Qaeda and mainly AQ inspired acts of terrorism, though the authorities appear to have the upper hand in this confrontation the spectre of the Abu Hafs al-Masri Brigade looms. In Eastern Europe, Russia and its regions, particularly the North Caucasus continue to be concerned with Chechen Terrorists, for example, the Caucasus Emirate and other Islamic separatist terrorist groups. During the Kosovo war the Kosovo Liberation Army was considered by some a terrorist outfit but by others a liberation movement. Beyond AQ and AQ inspired, individual atrocities are possible for example, the attacks in which Anders Behring Breivik, a Norwegian right wing fanatic, bombed government buildings in Oslo, killing eight, and then shot dead 69 people at a Labour Party youth camp on a nearby island. With Europe in the grip of austerity and countries like Greece in economic difficulties, terrorist reactionary groups have emerged for example so called anarchists in Greece continue to launch attacks against symbols of the state, for example, Revolutionary Struggle which followed the Revolutionary Organisation 17 November and Conspiracy of Fire Nuclei. In past decades in Europe, terrorist groups that were active included in Corsica, France, the Corsican Patriotic Front and Action Directe in France itself. In Germany the Baader-Meinhof Group also known as the Red Army Faction, the Communist Combatant Cells in Belgium and the Red Brigades in Italy. Elsewhere in Europe the peace process is holding up in Northern Ireland with only sporadic non-compliance by a small number of Provisional IRA diehards, like the splinter groups the Continuity IRA and the Real IRA other groups involved in the troubles were the Saoir Eire, the Irish National Liberation Army, the Cumann na mBan and Fionn Eireann and in response, on the other side, the Ulster Defence Association/Ulster Volunteer Force. ETA in Spain seems closer to embarking on a similar journey to that of the Provisional IRA, though this will appear to take longer to achieve.

Terrorism Finance

Terrorism Finance is like money laundering in someways but the underlying motives of those undertaking this activity is distinctly different even if the actual process is similar to those used by other criminals. Unlike criminal groups who primarily seek monetary gain, terrorist groups have non financial goals, such as publicity, dissemination of an ideology, the destruction of a society or regime, or simply spreading terror and intimidation. Terrorist groups may also compete with governments regarding their legitimacy and therefore are often unconcerned that their existence

and operations are visible to the public. Indeed this is one of the primary objectives behind their operations. In other respects terrorism financing aspects may mirror traditional Money laundering activity in that terrorist groups will co-mingle legitimately sourced funds with those sourced from criminal acts. The term “terrorism finance” is commonly used to describe a number of distinct types of activity and is best viewed along the lifecycle of money's involvement with terrorists. First, it can consist of the “raising” of initial funds for the ultimate benefit of the terrorist group itself or for a particular operation or type of terrorist activity. Secondly, once raised, the money's will need to be “moved” and then “stored” in a secure place and under the control of trusted persons connected to or acting on behalf of the terrorist group. Finally the funds will then be “used” to further the terrorist groups aims, which may include longer term investment, expenditure on day to day operations or in carrying out planned terrorist attacks.

Lifecycle View of Terrorist Financing				
	Raise	Move	Store	Use
Drug Trafficking	x			
Arms Trafficking	x			
Tobacco Smuggling	x			
Extortion	x			
Human Trafficking	x			
Kidnap and Hostage	x			
Murder and Bodily Harm	x			
Fraud	x			
State Sponsors	x			
Precious Metals	x		x	
Precious Stones	x		x	
Charities and NPO	x	x		
Money Service Businesses		x		x
Hawala		x		x
Banknotes	x	x	x	x
Wire Transfers		x		x
Cash Intensive Businesses		x		
Real Estate			x	
Source: Author				

The above chart seeks to illustrate by utilising this

Lifecycle view of terrorism finance how many of the more successful and well known terrorist groups have sought to “raise” funds largely through either, State sponsors, illicit activity (drug, weapons & tobacco trafficking, through precious metals and stones dealing, and through fraud, including credit card and similar and by kidnap and ransom, extortion and even by Bank Robbery as well as through charitable fund raising, funds moved through the use of wire transfers, money services businesses, informal value transfer services, charities & bulk cash smuggling, “store” monies by using precious metals and stones and bulk cash and “use” monies, via wire transfers, money services business, informal value transfer services & using bulk cash.

The chart provides a composite picture and does not reflect each terrorist groups terror financing activities per se. The way each is undertaken will be influenced by the culture and society within which the particular terrorist group operates and the skills and knowledge of those involved, against the activities of those seeking to interdict and disrupt those activities. For example, [Hamas](#) and [Hezbollah](#), both receive State and semi State support, usually in bulk cash and well as relying on charitable monies, [Al-Qaeda](#) has received funds disguised as charitable donations and has become involved in drug and weapons trafficking, precious metals and stones dealing, kidnapping and ransom. [Tamil Tigers](#) have relied upon charities but also extortion to obtain needed cash to support their activities. The [Irish Republican Army](#) were engaged in weapons dealing, extortion and bank robbery. The [FARC-ELN](#) trafficked in weapons and drugs as well as committed kidnapping and ransom in regions where there is a very formal banking sector, for example in North America and Europe, terror groups operating there have used banks to conduct wire transfers, in Central and South America, where money service businesses are tapped to assist in transferring funds between entities. In the Middle East and the greater Indian sub continent informal transfer systems such as hawala are regularly used to move money cross borders. Where precious metals and stones can still be traded and exchanged for example in Africa and some part of the Middle East and the Indian sub continent, terror groups operating there have used such valuables to conceal their money movement and the proceeds of their illicit activities. Perhaps the most common means to finance terrorist activities is simply cash, the most ubiquitous of products and the most useful in obtaining the goods and services needed to support their terror objectives. For more see Part 2, Section 5, Regions, Countries, Criminals & Terrorists and Part 2, Section 6, Terrorist Attacks.

Theft, Robbery & Trafficking

“A man who has nothing can whistle in a robber's face.”

Juvenal, Roman Poet active in the 1st and 2nd Century AD and author of “Satires”¹

Harms

Theft not only affects those who the crime is committed against but it affects the economy as a whole driving up prices of all goods. For example, a person walks into a grocery store and steals infant formula for her hungry baby. Weeks later the store owner conducts an audit of the inventory and discovers the theft that went unnoticed. In order to recover the losses from the theft, the store owner has no choice but to raise the price of baby formula thereby affecting all consumers.

Robbery, which is simply theft by force or the threat of force, has the same affects on society as theft. For example, a person is driving their car at night and comes to a red light. A criminal approaches the car with a weapon and demands the driver exit the car. The criminal enters the car and drives away robbing the individual of their personal property. However, all is not lost for the victim since auto insurance will most likely reimburse the victim of their stolen property. All consumers of auto insurance are victims since the insurance company will incur the loss. In order for the insurance company to recover the loss they raise the rate of insurance for all consumers.

Raising prices on common goods and services that people rely on because of theft and robbery obviously harms all consumers. Embezzlement is a type of theft that has a negative affect on the general public, especially when the funds being embezzled are public funds. A public official who is in a position of trust with public funds who embezzles robs all citizens from needed maintenance of public service infrastructure and necessary public projects that increase the standard of living of the community.

Statistics

The UNODC compiles statistics at the national level related to serious crimes including theft, robbery and motor vehicle theft. The statistics related to theft, robbery and motor vehicle theft are mostly comprised of developed countries with modern judicial systems and competent law enforcement, which would suggest accurate police reports and therefore accurate criminal statistics. The UNODC does not receive these statistics from many developing countries since in many

developing countries theft goes unreported to law enforcement resulting in statistics that are non-existent, greatly inaccurate or misleading.

The data below shows the US with the most occurrences of theft, more than three times the amount of the second country on the list, Germany. The US is also at the top of the list regarding motor vehicle theft. This may be a result of the amount of vehicles per capita in the US, which is one of the highest in the world, giving thieves a target rich environment to commit their crime. When looking at robbery statistics Mexico sits at the top of the list, which maybe a derivative of the escalating drug war in Central America.

Theft: (excludes burglary; housebreaking; robbery; and theft of a motor vehicle)		
Country	Number	
1 US	6,185,867	
2 Germany	1,833,293	
3 UK (Eng & Wales)	1,422,180	
4 Russian Federation	1,108,369	
5 Italy	944,025	
6 Netherlands	659,330	
7 Japan	612,115	
8 Canada	551,941	
9 Australia	461,169	
10 Sweden	367,965	

Source: UNODC 2010²

Robbery: (theft of property from a person with the threat of force)		
Country	Number	
1 Mexico	738,138	
2 Spain	528,063	
3 US	357,832	
4 Belgium	183,611	
5 Russian Federation	164,547	
6 Chile	81,667	
7 UK (England & Wales)	76,179	
8 Colombia	56,887	
9 Germany	48,166	
10 Italy	47,996	

Source: UNODC 2010³

Motor vehicle theft police-records	
Country	Number
1 US	737,142
2 Mexico	229,965
3 Italy	197,583
4 India	147,475
5 UK (England & Wales)	106,228
6 Japan	97,266
7 Canada	92,683
8 Germany	83,480
9 Spain	65,672
10 Australia	54,736

Source: UNODC 2010

Of all the thefts reported to police, identity theft is one of the most prominent types of theft in the world. According to a report by the UN Office on Drugs and Crime (UNODC) The Globalization of Crime: A Transnational Organised Crime Threat Assessment, more than 1.5 million people a year suffer the theft of their identity for an economic loss estimated at US\$1bio.⁴

In the US, identity theft has been the number one consumer complaint at the Federal Trade Commission (FTC), resulting in 19% of consumer complaints. Regarding the type of identity thefts that are reported to the FTC, government or benefit fraud is the number one type of identity theft. Credit card fraud is second on the list where identity thieves steal credit card numbers or open credit card accounts with stolen identities. For more details see Fraud above.

However shocking these statistics can be, the statistics related to retail theft can be just as shocking.

A report conducted by the UK-based Centre for Retail Research titled 2011 Global Retail Theft Barometer attempts to measure the cost of shrink (or leakage), which is a reduction in inventory due to shoplifting, employee theft, paperwork errors and supplier fraud. The study also attempts to measure how shrink affects the consumer. The 2011 report puts the global cost of shrink at US\$199.89 per family. When the cost per family is broken down by country, the statistics become much more staggering. For instance, shrink added US\$423 to the average American family's shopping bill in 2010 and US retailers lost almost US\$40bio in stolen goods, or 1.5% of the US retail sales in 2010.⁵

Definition / Description

Legal systems based on common law traditionally distinguish between theft (taking without consent) and fraud (obtaining with consent through deception), a distinction still preserved in many jurisdictions around the world. The two crimes are rarely regarded as mutually exclusive, and it is generally accepted that a crime may involve both theft and fraud (i.e., the theft and subsequent sale of an automobile).

There is no accepted, universal definition of theft or robbery. The UNODC defines each, however these definitions are used for statistical purposes. The generic definition of theft is when a person intentionally and fraudulently takes personal property of another without permission or consent and with the intent to convert it to the taker's use (including potential sale). Since tangible items can be stolen, intangible items can also be stolen, for example a person's identity.

Robbery is the same as theft but is an aggravated form of theft that involves violence or the threat of violence against a victim in his/her presence. Many criminologists have long regarded statistics on robbery to be one of the most accurate gauges of the overall crime rate. Robbery takes many forms, from simple crimes such as muggings to major ones, for example, art theft, jewel thefts and bank and other so called secure facility robberies.

Other terms must be acknowledged and defined to understand the full, criminal portrait of theft and robbery. As the theft and robbery of goods becomes more sophisticated, additional roles are incorporated in the crime. For instance, a person who knowingly initiates, organises, plans, finances, directs, manages, or supervises the theft of property for sale to others, or who knowingly traffics in stolen property, is guilty of trafficking of stolen goods. The term given to a person who traffics or buys stolen goods is commonly known as a fence. A fence is an individual who knowingly buys stolen property for later resale, sometimes in a legitimate market. The fence thus acts as a middleman between thieves and the eventual buyers of stolen goods who may not be aware that the goods are stolen. E-fencing is the sale of stolen or shoplifted items on the Internet (for example, a person who receives stolen goods from a thief and sells those stolen goods on eBay). Thieves commonly use fences to avoid the hassle and suspicion of selling directly to the final buyers of stolen goods.

Theft is also usually distinguished from embezzlement, in which the offender carries away goods the possession of which had been legally entrusted to him or her. As with fraud, theft is a separate crime from embezzlement,

but the two offenses are not mutually exclusive. Embezzlement may be one of the most detectable forms of theft since the individuals in a position to embezzle funds commonly do so via electronic fund transfers leaving paper trails for auditors to discover and law enforcement to follow.

History Background / Context

Theft and robbery are unfortunately as old as human history itself, are condemned in the ten commandments.

Punishment for theft and robbery was severe, with capital punishment or amputation, assault or imprisonment regularly meted out throughout the ages across many different cultures, and some of the first crimes to be noted in modern English law, in the twelfth century, to be one of a crime, made punishable by the state rather than through compensation of the injured party or through private vengeance. Robbery today, more often than not, carries more serious punishment since robbery involves violence or the threat of violence when stealing property.

In recent times thefts and robberies that have caught the most attention have been this carried out against Banks and secure establishments in order to steal Cash or other valuables such as jewellery and art. Some perpetrators have become notorious, others never caught but ball capture the public's imagination. Of course these include Butch Cassidy who in the US made headlines for robbing trains and ranches as well as Banks, for example, in 1889 at the San Miguel Valley Bank he made off with US\$20,000 in stolen cash.

In 1911, the world's most famous painting, the Mona Lisa, painted by Leonardo Da Vinci, was stolen from the Louvre in Paris by an employee and only recovered 2 years later. Vincenzo Peruggia had hidden in a broom closet, later taking the painting out of the frame and leaving after the museum was closed. Paruggia was an Italian patriot who believed the Mona Lisa should be returned to Italy, who was finally caught trying to sell the painting to the Uffizi Museum in Florence. Peruggia was still hailed as a hero in Italy, serving only 6 months in prison. The painting first toured Italy before being returned to the Louvre where it remains behind a protective and secure bulletproof glass.

In the 1930s arguably the most infamous bank robbers in history, Bonnie and Clyde, (Bonnie Parker and Clyde Barrow) carried out, according to the FBI a "violent crime spree across the Midwest that included auto theft, bank robbery, theft from the federal government, and the murder of more than a dozen people, including many law enforcement officers." following a national

manhunt both were gunned down and killed in 1934. The same year, another infamous bank robber John Dillinger was killed by Police after he and his gang robbed two dozen banks and four police stations. Since the gangsters and the gangs of the 1920s in the US caught the imagination, the limelight since has been shone on the biggest thefts and robberies since, carried out by organised gangs or terrorists, or professional thieves.

The following are considered the largest robberies by amount stolen.

Top Ten Robberies by amount stolen				
	Entity	Co	Date	Amt Stolen US\$mio
1	Central Bank of Iraq	Iraq	2003	US\$1bio
2	City Bonds Robbery	UK	1990	US\$400
3	Boston Museum	US	1990	US\$300
4	Baghdad Bank	Iraq	2007	US\$282
5	Schiphol Airport Heist	NL	2005	US\$118
6	Harry Winston / Jewellery Store	Fr	2008	US\$108
7	Antwerp Diamond Centre	Belg	2003	US\$100
8	Knightsbridge Security Deposit	UK	1987	US\$98
9	British Bank of Middle East	Leb	1976	US\$20-50
10	United California Bank	US	1972	US\$30 est

Source: <http://listverse.com/2009/12/01/10-largest-robberies-in-history/#comments>⁶

Whilst these are all large and significant the following are brief summaries of the top 10.

In what is now considered the largest bank robbery or theft in recorded history, Saddam Hussein's regime conducted a massive raid on **Iraq's central bank**. The day before Coalition forces began bombing Iraq, he sent his son Qusay to make a withdrawal on his behalf with a handwritten note. Qusay oversaw the withdrawal of boxes filled with US\$100 bills in a five-hour operation which is estimated at more than US\$1bio. Approximately US\$650mio was later found by US troops hidden in the walls of one of Saddam's palaces, though the remaining US\$350mio has never been recovered and is considered lost.

Second place involved John Goddard, a 58 year old messenger working for London financial intermediary, who was mugged whilst carrying a briefcase delivering £292mio in bearer bonds; Bank of England Treasury bills or equivalent to cash. Police believe that the **City Bonds Robbery** mugging was carried out by a low level thief brandishing only a knife on an insignificant back street, though that thief was found dead of a gunshot wound to the head before he could be charged and all but 2 of the bonds were recovered soon afterwards.

In third place, and also considered the biggest art robbery in history, was the robbery carried out at the Gardner **Boston Museum** in 1990, when two men dressed as police officers convinced 2 inexperienced security guards at the Gardner Museum that they were responding to a disturbance called in and in the process handcuffed the guards and then after selecting 12 pieces of art with a combined value of over \$300 million, they departed, never to be heard from again. Among the paintings stolen were 3 Rembrandts and a Vermeer.

In fourth place is another robbery in Iraq, this time post Saddam, at the **Baghdad Bank**, where it is believed that 3 guards at the bank made off with a US\$282mio. The culprits were never caught nor the money recovered.

In equal fifth place, at both just over US\$100mio, is first the largest diamond robbery in history, known as the **Schipol Airport Heist** where the thieves stole Dutch airline, KLM cargo truck and KLM uniforms and in February, 2005 took off with a KLM truck that was carrying a large haul of uncut diamonds intended for delivery to Antwerp. The thieves got away with an estimated haul of approximately US\$118 million. As many of the stones were uncut, this made them much harder to trace. In equal place, comes the robbery at **"Harry Winston" Jewellers** in Paris, where in December 2008, four armed men stole approximately US\$108mio of jewellery.

In seventh place is the robbery at the time dubbed the "heist of the century". The robbery took place in 2003 in the **Antwerp Diamond Centre**, by a 5-man Italian team known as "the school of Turin". Safe deposit boxes were forced open and gold, diamonds and other jewellery was looted, valued at more than US\$100mio. The gang was caught using DNA evidence from a found half eaten sandwich.

In eighth place, is the theft of safe deposit boxes in 2003 known as the **Knightsbridge Security Depot**, looting US\$98mio by Italian bank robber Valerio Vicci, who was later caught and sentenced to 22 years imprisonment, later shot and killed.

In ninth place, this time involving a terrorist group, is the **Palestine Liberation Organisation**, who in 1976 stole US\$20-\$50mio worth of jewels, gold, stocks and bonds from the **British Bank of the Middle East** in Beirut, a HSBC affiliate. This is not the first or last time that a terrorist organisation resorts to Robbery, for example see Part 2, Section 7, robbery of the **Northern Bank** by the **IRA**.

In tenth place, in 1972 the safe deposit vault at the **United Bank of California** was broken into by professional burglars led by Amil Dinisio, looting an estimated US\$12-30mio, being caught when a similar robbery with fingerprints left was linked.

Other famous robberies also include Stanley Rifkin's 1978, US\$10.8mio theft, described by TIME Magazine as "the ultimate heist", following the robbery at the **Security Pacific National Bank**, which at the time, stood as the biggest US bank robbery in history. This was topped by Allen Pace, in 1997 who stole US\$18.9mio and criminal mastermind behind the infamous, **Dunbar Armored Robbery**, the largest then cash robbery in US history. Pace was eventually captured and was sentenced to 17 years in prison.

Possibly the most famous robbery in UK history became known as the Great Train Robbery, here in 1963, 15 robbers attacked a mail train making off with £2.6mio (the equivalent of £46mio today).⁷

One of the most notorious specialized operations is known as the **Pink Panthers** international jewel thief network which is responsible for some of the most audacious thefts in criminal history, including the robbery of the jewellery store Harry Winston in Paris, in December 2008, where they escaped with more than €80mio worth of jewellery. They are responsible for what have been termed some of the most glamorous heists ever, with their crimes being thought of as "artistry" even by criminologists. They have targeted several countries and continents, and include Japan's most successful robbery ever amongst their thefts. Interpol believes that the group are responsible for more than 341 cases since 1999 worth in excess of €330mio.

Money Laundering

High value theft or robbery, for example, the theft of high valued art, precious metals or stones or large scale bank robberies, usually involve organised criminal gangs, terrorist organisations or sophisticated criminals who have access to or methods of disposing of their theft and exchanging it for less traceable assets.

Of the largest robberies and thefts, those that were well

planned and highly organised have been successful and much of the loot remains unrecovered. It is extremely unlikely that robbers and thieves would try to bank their ill-gotten gains, with immediate red flags being raised and the consequences for them as a result. For more simple, thefts, cash or property is more likely used and or exchanged via online auction sites though most often on the black market, using intermediaries and or contacts or known "fences."

Aside the grand robberies and major thefts and the petty thefts, are a number of systematic thefts that generate significant criminal proceeds and attract organised and criminal gangs as well as the more opportunistic criminal. These are Identity Theft and Motor Vehicle Theft.

Bank Robbery

Whilst, bank robbery methods are as novel and varied, the most common approach is to step up to a bank teller and make a demand verbally, with a written note, or both, at least in the US, according to the FBI. In the USA for 2008, this technique was used in 3,833 of the 6,700 bank robberies that year. Weapons were threatened in roughly a third of robberies and used in about one in four. Interestingly, again according to US data, robberies most often occur on Fridays and between 9 and 11 a.m. The FBI have a clean up rate of approx 50%

Identity Theft

There are many types of Identity theft including those targeted towards obtaining bank account or credit and debit card details (See Fraud above for details). Nevertheless the most pervasive type of identity theft fraud relates to benefit and entitlement fraud. This fraud occurs when identity thieves use a stolen social security number or similar ID and apply for government benefits or entitlements.

Motor Vehicle Theft

Criminal gangs are known to find cars, particularly attractive and have developed intricate operations, with multiple layers and multiple individuals who participate in the crime. The first layer of the criminal operation is the actual theft of the motor vehicle. The stolen vehicle is then sold to a fence who has the VIN (vehicle identification number) altered and creates a fraudulent Certificate of Title for the stolen vehicle so that it matches the altered VIN. This is done to avoid detection by law enforcement. The fence then sells the stolen vehicle, either domestically or overseas, to a buyer. The funds of these transactions must be laundered in order for the fence to be successful. This may be done by using shell companies or co-mingling the funds from the

criminal racket with a legitimate, cash intensive business the fence may own or have access to. Those stealing the cars and the fence and the buyer may in many cases be closely or more loosely connected or affiliated to a particular criminal gang. Major markets for car thefts include the UK, Netherlands and Germany with then transit routes east including through the Baltic States and the Balkans elsewhere to Eastern Europe and from the US through Mexico and into Latin America.

Beyond theft and smuggling to new markets, commercial Vehicle theft operators may also engage in Stripping Operations, to respond to the demand for cheap used component parts to repair damaged vehicles, where the supply of salvage vehicles available is outstripped by demand. For some the desire to shortcut the process by obtaining parts etc that are already the right color increases their profit margin. Thefts based on orders for specific parts by make, model, and color are not unusual.

And then there is Insurance Fraud, with some estimates that 30% or more of all insurance claims involve some type of fraud. Offenders in this category range from individuals that inflate their claim to organised rings that dispose of vehicles or stage auto accidents among themselves or involving innocent drivers. Inflated and fraudulent insurance claims cost the average driver dearly in premiums.

Other reasons that cars are stolen include joyriders, those about to commit another crime, for example criminals use stolen vehicles for everything from transporting drugs and transportation for robberies and drive-by shootings.

WMD Proliferation Finance

"Proliferation of nuclear weapons to terrorist organisations is far more dangerous than proliferation of nuclear weapons to states, even states like North Korea."³

John Bruton, Irish Prime Minister from 1994-1997¹

Harms

There is little dispute that Weapons of Mass Destruction, or WMD, pose a grave threat to global security and to human life if they fall into irresponsible hands. Whether nuclear, chemical or biological, the consequences could be devastating and so ensuring non-proliferation is essential.

Furthermore it is where Terrorism and WMD Proliferation come together that the real prospect potential for actual harm on an almost unimaginable basis provides greatest concern.

This is why Rogue States engaged in developing WMD cause great concern. Whilst the traditional view of terrorism was that terrorists would seek to limit casualties so as to make an impact but not to cause an excessive damaging response, the events of 9/11 changed that view. Though the traditional view may still hold for the majority of the major terrorist organisations, Al-Qaeda has clearly departed from it and only the complacent would consider them as either a spent force or unwilling if it had the means, to use WMD.

As Rogue States are the most likely conduit to Terrorists getting their hands on such weapons it is essential that a strong WMD proliferation Finance regime is in place and is fully supported.

Statistics

Estimates of casualties from chemical weapons in the First World War vary but were likely almost 90,000 dead and 1.2 million injured.²

To appreciate the devastation of nuclear weapons, the examples of Hiroshima and Nagasaki are the only ones available. Over 185,000 people were killed more than half instantly and the rest over time through the effects of the blasts and the effects of radiation.³

The Halabja poison gas attack was a massacre against Iraqi Kurds by the regime of Saddam Hussein, during the closing days of the Iran Iraq war. The attack is estimated to have killed between 3,200-5,000 and injured around 7,000-10,000 more.⁴

According to the IAEA Illicit Trafficking Database, between 1993 and 2007 there was 1,340 confirmed incidents of nuclear and radioactive material trafficking in the world.⁵ Also IAEA have reported 2,200 recorded attempts of smugglers attempting to steal uranium between 1995 and 2012. In order to create a dirty bomb, at least 55 pounds of highly enriched uranium is needed.

Definition / Description

Proliferation Financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations (provisional FATF definition). Without safeguards such funds and services can become accessible to individuals and entities seeking to profit from the acquisition and resale, or even reach terrorists. Proliferators mask their acquisitions as legitimate trade and exploit global commerce for example by operating in countries with high volumes of international trade or utilising free-trade zones, where their illicit procurements and shipments are more likely to escape scrutiny. Proliferation networks work to conceal the end-user of traded goods, the goods themselves as well as the entities involved and associated financial transactions. To ensure that the real end-use of sensitive goods being exported is not detected by authorities, the networks may use intermediaries and front companies to arrange the trade or export of goods and those may use fraudulent documents, such as false end-use certificates, forged export and re-export certificates. Facilitators such as couriers may be used to ensure that the transfer of goods avoids inspection to ensure the safe entry of the goods.

The FATF established Typologies Report on Proliferation Financing providing further details and listing elements that may indicate proliferation financing. The FATF also established a status report on the policy development and consultation of Combating Proliferation Financing.⁶

Weapons of Mass Destruction are essentially those weapons that are designed to release chemical toxins, biological agents or nuclear radiation that can kill indiscriminately or can endanger significant numbers of lives, or cause a major impact on property and/or infrastructure. WMD proliferation is the illegal transfer and export of nuclear, chemical or biological materials

and/or weaponry and/or their means of delivery.

There are currently 8 or perhaps 9 States that possess nuclear weapons or have nuclear weapons capabilities. These are the 5 permanent members of the UN Security Council, US, Russia, UK, France and China, as well as more recent acquirers, India and Pakistan, the Rogue State of North Korea and almost certainly Israel, though it has refused to confirm or deny this. It is also widely suspected that Iran is close but has not yet acquired nuclear weapons, that South Africa had but no longer maintains the capabilities and that Iraq and Libya unsuccessfully attempted to acquire nuclear weapons.⁷ Iraq certainly tried to build a nuclear weapons programme though by the time of the lead up to the second Gulf War it had given up its attempt, though western intelligence agencies famously got this wrong. Libya seeing the writing on the wall after 9/11 brokered a deal to close its programme in exchange for normalising relations with the West.

Nuclear States	
1	US
2	Russian Federation
3	China
4	France
5	UK
6	India
7	Pakistan
8	Israel (Israel still refuses to confirm);
9	North Korea

Source: Inst for Science and Int Security

The Nuclear Non-Proliferation Treaty 1970 (NPT), is based on a central bargain that the NPT Non nuclear weapon States agree never to acquire nuclear weapons and the NPT nuclear Weapons States agree in exchange, to share the benefits of peaceful nuclear technology and to pursue disarmament aimed at the ultimate elimination of their arsenals.

Countries Sought / Seeking Nuclear Weapons	
1	South Africa (dismantled)
2	Libya (Sought & dismantled)
3	Iran (Seeking)
4	Syria (unclear)

Source: Inst for Science & Int Security

Whilst in the area of nuclear weapons, the Nuclear Non-Proliferation Treaty 1970 applies, other treaties apply to biological and chemical weapons. The Biological Weapons Convention 1972 was the result of prolonged efforts by the international community to extend the prohibition already on use of biological weapons, contained in the 1925 Geneva Conventions, to cover also possession and development. The Chemical Weapons Convention 1993 essentially mirrors the BWC, but also provides for the destruction and verification thereof of all Chemical stockpiles.⁸

As of November 2011, around 71% of the declared stockpiles⁹ of Chemical Weapons had been destroyed. Several countries, that are not members are suspected of having Chemical Weapons, especially North Korea and Syria, whilst others including Sudan are accused by some of not declaring accurately their stockpiles. Russia & the US, the 2 countries with the largest declared stockpiles, are in the process of destroying them, with the former at around 57% and the latter at 90% completed.¹⁰

Historical Background / Context

Simple forms of biological warfare have been used throughout history, for example during the 6th Century BC, the Assyrians poisoned enemy wells with a fungus. Hannibal, the great General and scourge of Rome in 184 BC, filled pots with snakes to throw onto the decks of enemy ships during close battle. In the Middle Ages, during the time of the plague, Mongol and Turkish armies were reported to have catapulted disease ridden corpses into besieged cities, later copied in 1710 by the Russians against the Swedes in Tallinn.¹¹

The British tried to use smallpox as a weapon when they gave contaminated blankets to the Native Americans during hostilities in 1763.

At the end of the 19th Century, with the development of science and the increasing understanding and expertise of chemists, concerns about the potential use of Chemical Weapons were raised resulting in the signing of the Hague Convention in 1899 where signatories agreed not to use projectiles whose sole purpose was the diffusion of toxic gas.

With the onset of the First World War in 1914 the Convention would get its first major test. With the battle deadlocked in France, Germany contemplated using Poison Gas to break the stalemate. Not wanting to be the first to break the Convention however they first blamed the French, who they claimed were using a new type of weapon, essentially gas grenades which once exploded giving off lethal fumes. In response and using

this pretext as justification the Germans launched a chlorine ("Mustard Gas") attack at Ypres in 1915, causing general outrage and shocking the world. The Allies would soon respond in kind but throughout the war were generally lagging behind the Germans in the development of new and more dangerous chemical weapons. Estimates of casualties from chemical weapons vary but likely resulted in 90,000 deaths and 1.2 million injured.¹² The largest attacks by far were inflicted by the Germans on the Russians who accounted for around half in each category, though in context this was still a relatively small amount, approximately 4% of the total dead or injured. The Germans also tried to use anthrax to little effect during the First World War.

In World War 2, Japan used biological weapons on Chinese soldiers and civilians, deploying plagued foodstuffs which may have infected over 500,000 people. In response to Nazi Germany which was suspected of developing biological weapons, the Allies produced but never deployed biological weapons, including anthrax toxins, which were tested and left one Scottish Island contaminated for the next 50 years.

In order to finish the Second World War, to avoid the loss of further Allied lives preparing to invade Japan and to persuade the Japanese Military to surrender, the US dropped atomic bombs on Hiroshima Japan on 6 August 1945, instantly killing 60,000-80,000 Japanese citizens, Koreans who had been forced to come to Japan as labourers, and American prisoners-of-war who were imprisoned in Hiroshima. The blast destroyed more than ten square kilometers (six square miles) of the city. The intense heat of the explosion then created many fires, which consumed Hiroshima and lasted for three days, trapping and killing many of the survivors of the initial blast. In all 135,000 would lose their lives with many dying from radiation sicknesses. On 9 August 1945, the Americans dropped a second, more powerful atomic bomb, on Nagasaki, an important Japanese port, which killed 40,000 people instantly and another 10,000 from radiation sicknesses. On 14 August 1945, Japan agreed to the Allies' terms of surrender. At midday on the following day, Emperor Hirohito broadcast the news to the Japanese people. It was the first time his voice had been heard on the radio.¹³

Whilst the US hoped to maintain a monopoly on its new weapon and to keep secret the methods for making nuclear weapons, it took only four years before the Soviet Union detonated its first nuclear device. The UK followed in 1952, France in 1960 and China in 1964. Seeking to prevent the nuclear weapon ranks from expanding further, the US and other like-minded states negotiated the nuclear Non-Proliferation Treaty (NPT).

1970.¹⁴

In the decades since, several states have abandoned nuclear weapons programmes, but others have defied the NPT. India, Israel, and Pakistan have never signed the treaty and possess nuclear arsenals.¹⁵ Iraq initiated a secret nuclear programme under Saddam Hussein before the 1991 Persian Gulf War. North Korea announced its withdrawal from the NPT in January 2003 and has tested nuclear devices since that time. Iran and Libya have pursued secret nuclear activities in violation of the treaty's terms, and Syria is suspected of doing the same. Still, nuclear non-proliferation successes outnumber failures and dire forecasts decades ago that the world would be home to many dozens of states armed with nuclear weapons have not been realised.

The Halabja poison gas attack in 1988 was a massacre against Iraqi Kurds by the regime of Saddam Hussein during the closing days of the Iran-Iraq war. The attack is estimated to have killed between, 3200 and 5000 and injured between 7,000 - 10,000 more. This genocidal act remains the largest chemical weapons attack directed against a civilian population in history. The Iraqi regime dropped bombs by fighter planes on the Kurdish Town of Halabja, with numerous cocktails of chemicals. It is believed that mustard gas as well as sarin and other chemical weapons were used, inflicting terrible deaths and injuries on its victims.

In 1995, during the morning rush hour in Tokyo, sarin gas was released on 3 subway trains, affecting 5,000 passengers, injuring hundreds and killing 8. No one claimed responsibility for the attack, which completely terrorized Tokyo residents, though soon Japanese investigators began carrying out raids on a strange religious group called Aum Shinrikyo which had believed the world was coming to an end. Investigations uncovered several tons of chemicals, some of which could be used to create sarin, gas masks and approximately US\$7mio in cash. At one location, officials found fifty drums containing phosphorus trichloride, a required ingredient for making sarin gas. It was estimated that Aum Shinrikyo had enough chemical materials to kill more than 4 million people.¹⁶

After the September 11 terrorist attacks, where the attacks themselves caused massive loss of life, there were increased concerns about Rogue States as well as black market networks and terrorist groups obtaining WMD and related components, particularly from ex-Soviet countries where controls over stockpiles and materials were considered by many to be negligible.

According to Pulitzer prize winning author, Ron

Suskind in his book "The One Percent Doctrine,"¹⁷ published in 2006, he ascribes to Vice President Dick Cheney an operating principle articulated shortly after 9/11. According to Mr. Suskind, "if there was even a 1% chance of terrorists getting a weapon of mass destruction — and there has been a small probability of such an occurrence for some time — the US must now act as if it were a certainty," and argues that this conviction effectively sidelined the traditional policymaking process of analysis and debate, making suspicion, not evidence, the new threshold for action and as the basis for the decision to invade Iraq in 2003. Mr. Suskind's book also revealed that Al-Qaeda operatives had designed a delivery system (which they called a "mubtakkar") for a lethal gas, and that the US government had an Al-Qaeda source who said that plans for a hydrogen cyanide attack on New York City's subway system were well under way in early 2003, before the attack was called off. The book also reports that Al-Qaeda had produced "extremely virulent" anthrax in Afghanistan before 9/11 which "could be easily reproduced to create a quantity that could be readily weaponised."

In September 2007, Israel conducted an airstrike on what US officials have alleged was the construction site of a nuclear research reactor. Subsequent International Atomic Energy Agency (IAEA) investigations into the US claims uncovered traces of undeclared man-made uranium particles at both the site of the destroyed facility and Syria's declared research reactor. Syria is thought to have obtained crucial nuclear information from North Korea.

In its 2008 report World at Risk, the Commission on the Prevention of WMD Proliferation and Terrorism¹⁸ stated there is a high likelihood of some type of WMD terrorist attack by the year 2013.

In 2012, Syria admitted to possessing a stockpile of chemical weapons and has been accused of deploying these weapons in the course of the Syrian Civil War that rages on. Syria is one of five states that have not signed and seven that have not ratified the Chemical Weapons Convention, which prohibits the development, production, stockpiling, transfer, and use of chemical weapons. Syria is thought to have the third largest stockpile of Chemical weapons. In the area of Ghouta an alleged Assad government chemical weapons attack caused the deaths of hundreds to 1,400 people. Western intelligence agencies have long accused the Syrian regime of using chemical weapons on numerous occasions since 2012 with the latest in August 2013, in the area of Ghouta.¹⁹

Money Laundering

FATF issued a well publicized Proliferation Financing Report in 2008 which discussed the link between financial services and the transfer of WMD. As FATF points out in its report, the complexity of procurement networks has increased, and the number of actors involved in transactions has also increased. Transactions involving multiple parties and transfers of ownership may disguise the true nature of a transaction. While proliferation rings operate globally, government controls are by no means uniform, creating weaknesses that can be exploited. Companies have used a variety of means to evade export restrictions and sanctions filters. Front companies can be used to hide the ultimate end user of a product. One method is the use of a front company to receive the goods and reroute them. Intermediaries are also used. Where goods are transported to a front company in a third jurisdiction, an intermediary is used to obtain the required export licenses for further transport to a proliferator, often by forging an end user statement, falsifying shipping documents or through bribery.

The FATF report discussed a trend toward selling more elementary components – many of which could have multiple uses and might not even be controlled by export authorities. Even if detailed information on a goods shipment is available, highly specialized knowledge is needed to determine if a good is used in proliferation. Finally, transaction parties can conceal the nature of the good shipped and its ultimate application/use by creating fraudulent descriptions.

Some of these disguises and manipulations can be found in the activities of Abdul Qadeer Khan, a Pakistani Nuclear Scientist credited with providing Pakistan with its nuclear weapons. In 2004 Khan confessed to heading a clandestine group that supplied Pakistani nuclear technology to sanctioned countries. Khan admitted to having provided Iran, Libya, and North Korea with designs and centrifuge technology to aid in nuclear weapons programmes. Another example is the case of Li Fang Wei (aka Karl Lee), a Chinese citizen, and his company who helped supply Iran with goods needed for its nuclear and WMD development. The Manhattan District Attorney's Office, working closely with OFAC, charged Lee with misuse of Manhattan banks and the proliferation of illicit missile and nuclear technology to the Government of Iran. In doing so, the MDA drew parallels to its earlier pursuit of financial institutions engaged in payment stripping.



Section 2 - Money Laundering Risks

1. Money Laundering Risks

Money Laundering Risks Identified, 131

- Financial Action Task Force, 131
- United States, 133
- European Union, 134
- Other Countries, 134
- The Wolfsberg Group, 134
- Additional Sources, 135

4. Country Risks

- Country Risk Methodology & Sources, 215
- Financial Action Task Force/FATF, 215
- Sanctioned Countries, 216
- Wolfsberg Group, 217
- Basel Institute of Governance, 218
- Additional Methods & Sources, 218
- Hot Spots (in-Country and Regional, 221
- Diversion Risk or Close Proximity Risk Countries, 221
- Free Trade Zones, 222
- Time Zone Risk, 222

2. Customer Risks

- Arms Dealers, 139
- Banks & other Financial Institutions, 141
- Cash-Intensive Businesses, 143
- Casinos including Internet Gambling, 145
- Charities & Not For Profit Organisations, 152
- Gatekeepers, 154
- High Value Goods Dealers, 157
- Intermediaries, 161
- Money Service Businesses, 162
- Politically Exposed Persons, 166
- Precious Metals & Stones Dealers, 169
- Private Military Firms, 173
- Real Estate Agents, 175

3. Products & Services (incl Channels) Risks

- A Brief History of Banking, 179
- Asset Management, 181
- Brokerage / Securities, 183
- Commercial Banking, 186
- Correspondent Banking, 191
- Credit & Other Cards, 198
- Investment Banking, 201
- Retail Banking, 205
- Wealth Management/Private Banking, 209

Sub-section 1. Money Laundering Risks



Money Laundering Risks Identified, 131

- Financial Action Task Force/FATF, 131
- United States, 133
- European Union, 134
- Other Countries, 134
- The Wolfsberg Group, 134
- Additional Sources, 135



- Customer Risks
- Product & Services Risks
- Channels Risks
- Country Risks
- Transaction Risks
- Money Laundering Crimes
- Money Laundering Laws & Regulations
- Money Laundering Prevention Programmes

Money Laundering Risks Identified

Whilst all financial institution customers, products and services, channels of distribution and geographies present some kind of inherent money laundering risk, there are particular ones that present increased inherent risks. There are also others where risks can be considered as reduced.

FATF and others, including the US, the EU and the Wolfsberg Group have identified particular customer categories or situations, products and services including the channels by which they can be accessed and geographies that may pose additional inherent money laundering risks, as well as some that may present lower risks.

This Sub-section contains specific information from FATF, the US and the EU and then from the Wolfsberg Group before a summary of the responses developed by UBS both to the specific risks identified, UBS Customer/Product Risk Methodology and Response and the most important measures employed in response, for first Customers and then Products and Services.

Then Sub-section 2 focuses on the main customer types that pose increased risks and Sub-section 3 analyses the core products and services via the main business operations conducted by financial institutions. For each of these major lines of business, the most important risks are identified as well as potential channels or distribution risks as appropriate alongside key scenarios identified that pose the greatest risks and should be considered to be addressed.

Sub-section 4 deals with geographies or country risks, looking at methodologies, examples and many of the most important sources, in order to identify relative risk classifications between countries.

Financial Action Task Force/FATF

The customer segment that has a high inherent risk not usually due simply to itself but its own customers and is most highly regulated are of course financial institutions themselves, including **banks, brokerages, insurance companies, credit, mortgage and other finance houses**. FATF identify in particular **correspondent banking** including **wire transfers** and **money or value transfer services** and **cash couriers**, who move cash and other bearer negotiable instruments cross border, as demonstrating particular risks and requiring additional preventative measures, as well as requiring financial

institutions to consider the risks and take appropriate measures with respect to new products and/or new technologies for both pre existing and new products. These financial institutions are charged to maintain the integrity of the financial system.

Beyond financial institutions, FATF have identified other Categories of increased risks, most notably **Politically Exposed Persons**, who are seen as particularly at risk of Corruption and **Charities and Not for Profit Organisations** at risk for Terrorism Finance.

FATF mentioned risks or risk categories to be addressed	
1	Banks and other FIs incl MSBs / Correspondent & Private Banking
2	PEPs
3	Charities and NPOs
4	Lawyers, Accountants and Company Service Providers
5	Real Estate Agents
6	Precious Metals and Stones Dealers
7	Casinos

Source: Author

FATF have also identified another class they call, **Designated Non-Financial Professions and Businesses (DNFPBs)** being professions and businesses that are seen as being attractive to money launderers and these are: **casinos**, (when their customers engage in financial transactions above US\$3,000), **lawyers, accountants and trust and company service providers, dealers in precious metals and stones** (when their customers engage in cash transactions above US\$15,000) and **real estate agents**.

Beyond DNFBPs FATF have also identified other groups or situations where the risk of money laundering or terrorist financing is potentially higher, and enhanced measures have to be taken, in particular by financial institutions where customers (i) **conduct their business relationship in unusual circumstances** (got example, significant unexplained geographic distance between the financial institution and the customer); (ii) are **non-resident customers**; (iii) are **legal persons or arrangements that are personal asset-holding vehicles**; (iv) are **companies that have nominee shareholders or shares in bearer form**; (v) are **businesses that are cash-intensive**; (vi) have an

ownership structure with a company that appears unusual or excessively complex

given the nature of the company's business; and (vii) have **significant country or geographic risk factors**, in particular

- (a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems and/or where counter measures have been called for
- (b) Countries subject to sanctions, embargoes or similar measures issued by, for example, the UN;
- (c) Countries identified by credible sources as having significant levels of corruption or other criminal activity; and
- (d) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist groups operating within their country. For more details about Country Risks see Part 1, Section 2, Sub-section 4 below; Section 4, Sanctions and Embargoes as well as Section 5, Criminals and Terrorists by Region and Country; Section 6, Terrorist Attacks and Section 7, Criminal Cases which have significant country connections.

FATF mentioned risks or risk categories that MAY need to be addressed	
1	Customers conducting business in unusual circumstances
2	Non-resident customers
3	Personal investment company customers
4	Nominee companies or bearer share companies
5	Unnecessarily unusual or complex customer ownership
6	Customers with significant country risk exposure
7	Non-face-to-face relationships/transactions
8	Payments received from unknown or third parties

Source: Author

Where once the visit to the bank would have required a visit to a market square, where the customer could find his banker sitting at a bench or counter (In Italian 'banco' and German 'bank'; both meaning bench or counter), today, customers have a plethora of alternatives to access their bank, including visit to traditional bricks and mortar branches, to use of mail and other physical delivery options, ATM machines, telephone banking, video banking, mobile and online banking. For VIP Customers, private bankers for example or business banking, will often visit customers at their homes or businesses. For other customers or those wishing a less intimate experience, new methods

to access products and services and indeed the design themselves of certain products and services may present risks as a result and therefore FATF go beyond specific customer types and have identified the following as posing potential increased risks: (i) **Private Banking**; (ii) **Anonymous transactions** (which may include cash); (iii) **Non-face-to-face business relationships or transactions** and (iii) **Payments received from unknown or unassociated third parties as particular product, service, transaction or delivery channel risks**.

Finally FATF through its typology, trends and ad hoc other work has focussed on some of the above as well as additional areas of perceived money laundering and terrorism financing risks (beyond predicate offences themselves) and published reports which validate and/or indicate new areas of potential increased risks in the following customer related areas: 2010 - "**Money Laundering Using Trust and Company Service Providers (TCSPs)**"; "**Money Laundering Using New Payment Methods**," which compared the "potential risks" described in the 2006 report on New Payment Methods to the "actual risks" based on new case studies and typologies; "**Money Laundering through Money Remittance and Currency Exchange Providers**," which set out identified money laundering and terrorist financing methods and techniques involving money remittance and currency exchange providers; and "**Money Laundering vulnerabilities of Free Trade Zones**," where concerns have been raised about illicit actors taking advantage of more relaxed oversight to launder the proceeds of crime and finance terrorism highlighting the vulnerabilities of free trade zones.

2009: "**Money Laundering and Terrorist Financing in the Securities Sector**", which studied (i) how criminals might be able to use securities firms to launder money and finance terrorism and (ii) how illicit funds can be generated through fraudulent activities; "**Money Laundering through the Football Sector**", where several case examples of areas that could be exploited by those wanting to invest illegal money into football were described with concerns raised about the risks facing the football sector in particular and the sports industry in general to misuse by criminals; and "**Vulnerabilities of Casinos and Gaming Sector**", which included typologies and also considered vulnerabilities. 2008: "**Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems**", which focused on mediated customer-to-customer websites as the most vulnerable to abuse because of their popularity, accessibility (to the public), and high volume of cross border trade transactions, including a number of case studies 2007: "**Money Laundering and Terrorist**

Financing Through the Real Estate Sector”, exploring how illicit money may be channelled through the sector to be integrated into the legal economy and identifying some of the potential control points that could combat this; “**Laundering the Proceeds of VAT Carousel Fraud Report**”, which investigated the characteristics of the money laundering cycle from the proceeds of the fraud to investment into the legitimate economy as well as potential methods of prevention; and “**The Misuse of Corporate Vehicles, Including Trust and Company Service Providers**”, which used cases studies to illustrate the misuse of corporate vehicles, showing key elements and patterns. 2006: “**Report on New Payment Methods**” which reviewed a number of payment methods to identify trends and assess the vulnerabilities to money laundering and terrorist financing. 2004: ‘**Combating the Abuse of Alternative Remittance Systems (SR VI) Best Practice, alternative remittance**”, which provided guidance on how to detect alternative remittance systems outside the conventional financial sector, and “**Best Practice, cash couriers, bearer negotiable instruments, SR IX**”, which provided best practices for the areas that have proven most challenging. 2002: FATF issued “**International Best Practices: Combating the Abuse of Non-Profit Organisations (SR VIII)**”, which included guidance that would best aid authorities to protect non-profit organisations that engage in disbursing funds.

According to FATF (Interpretative Note on Recommendation 10 - Customer Due Diligence) there are circumstances where the risk of money laundering or terrorist financing may be lower, for example: (i) **financial institutions and DNFBPs** – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements; (ii) **Public companies** listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership; (iii) **Public administrations or enterprises** though there may be product, service, transaction or delivery channel risk factors; (iv) Life insurance policies where the premium is low (for example, an annual premium of less than US\$1,000 or a single premium of less than US\$2,500); (v) **Insurance policies** for pension schemes if there is no early surrender option and the policy cannot be used as collateral (vi) A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of

deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme; (vii) Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for **financial inclusion** purposes.

FATF - mentioned excessive risks or risk categories	
1	Shell Banks
2	Unregulated MSBs
3	Iran/North Korea
4	Anonymous Transactions
Source: Author	

United States

Outside of FATF, the US, as can be seen in the FFIEC Bank Secrecy Act/Anti-Money Laundering Manual, have identified the following customer types as posing special risks, requiring financial institutions to take these risks into account in their money laundering prevention programmes. These are: (i) **Foreign financial institutions**, including **banks and foreign money services providers** (for example, casas de cambio, currency exchanges, and money transmitters); (ii) **Non-bank financial institutions** (for example, money services businesses; casinos and card clubs; brokers/dealers in securities; and dealers in precious metals, stones, or jewels); (iii) **politically exposed persons (PEP)**; (iv) **Non-resident alien (NRA)** and accounts of foreign individuals; (v) **Foreign corporations and domestic business entities**, particularly offshore corporations (such as domestic shell companies and **Private Investment Companies (PIC)** and **international business corporations (IBC)** located in higher-risk geographic locations; (vi) **Deposit brokers**, particularly **foreign deposit brokers**; (vii) **Cash-intensive businesses** (for example, convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages); (viii) **Non-governmental organisations and charities (foreign and domestic)** and (ix) **Professional service providers** (e.g. attorneys, accountants, doctors, or real estate brokers).

According to the US Bank Secrecy Act/Anti-Money Laundering Manual, a number of products and services offered by banks may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes

of currency or currency equivalents. These include: (i) **Electronic funds payment services — electronic cash** (for example, prepaid and payroll cards), **funds transfers (domestic and international)**, **payable upon proper identification (PUPID) transactions**, **third-party payment processors**, **remittance activity**, **automated clearing house (ACH) transactions**, and **automated teller machines (ATM)**; (ii) **Electronic banking**; (iii) **Private banking (domestic and international)**; (iv) **Trust and asset management services**; (v) **Monetary instruments**; (vi) **Foreign correspondent accounts** (e.g. bulk shipments of currency, pouch activity, payable through accounts (PTA), and US\$ drafts); (vii) **Trade finance**; (viii) **Services provided to third party payment processors or senders**; (ix) **Foreign exchange**; (x) **Special use or concentration accounts**; (xi) **Lending activities**, particularly loans secured by cash collateral and marketable securities; and (xii) **Non-deposit account services** (for example, **non-deposit investment products and insurance**). FINCEN in the US also issue regular “Advisories” to domestic US financial institutions on money laundering and terrorist financing risks, on for example: 2012: **Third Party Payment Processors; Foreign Located Money Services Businesses**; 2010: **Informal Value Transfer Systems**; 2009: **Casino Patrons and Personnel**; 2008: **Casinos and Card Clubs; Foreign PEP's**; 2003: **Informal Value Transfer Systems**; 1999: **Black Market Peso Exchange**.

US mentioned risks or risk categories (Federal Exam Manual)	
1	Foreign FIs incl foreign banks and MSBs
2	Non-bank FIs incl MSBs
3	Casinos and card clubs
4	Brokers/Dealers in securities
5	Precious metals, stones or jewels
6	PEPs
7	Non-resident aliens
8	Foreign Corps/Domestic Shell companies - PICs / IBCs in higher risk locations
9	Deposit Brokers, particularly foreign deposit brokers
10	Cash Intensive Businesses
11	Charities and NGOs
12	Professional Service Providers (attorneys, accountants, doctors or real estate brokers)
Source: Author	

European Union

The EU in its Third Money Laundering Directive 2005 also include a broad category of dealers who trade in goods (but not services), where payments in cash are made in excess of €15,000, which are now known as **High Value Goods Dealers**, which was intended to cover some of the above FATF requirements on DNFBPs and others for example, art dealers and auctioneers, plane, boat, automobile, wine, watch and other high end **dealers**. Switzerland in its Anti Money Laundering Ordinance 2009 also includes “**Professional Banknote Dealers**”, non-banking institutions (companies or individuals) either within or outside Switzerland, which are engaged in buying or selling Banknotes and earn significant income or revenues from such activities.

Other Countries

Some other countries are also of interest, where there may not be a specific mention in legislation/regulation about heightened risks of an industry. In Switzerland, for example, whilst a number of industries are highlighted as being of higher money laundering risk, there is no specific mention of Charities, Auction Houses, Art Dealers, Cash Intensive Businesses or, for example, Sovereign Wealth Funds. **Canada** takes a similar approach to **Switzerland** with the exception of Canada not recognising complex structures specifically as an area of heightened risk but recognising Cash Intensive Businesses as being of heightened risk. Also, Canada mentions the issuance of bearer shares and companies using trade finance services as presenting increased money laundering risk. **Hong Kong**,

Singapore and **Australia** share a similar view on risks, with some notable exceptions: Australia does not specifically recognise Money Services Businesses or Intermediaries as being of increased risk; and Singapore does not specifically recognise Complex Structures as potentially increasing risks. The **UK** goes further than the EU in some respects by considering auction houses, art dealers, arms dealers as presenting increased risks unlike the EU.

The Wolfsberg Group

The Wolfsberg Group in its “Guidance on a Risk Based Approach for Managing Money Laundering Risks,” identified a number of customer groups that may pose higher risks. These are: “**Armament manufacturers, dealers and intermediaries; Cash (and cash equivalent) intensive businesses including: money services businesses (remittance houses, exchange houses, casas de cambio, bureaux de change, money transfer agents and bank note traders); casinos, betting and other gambling related activities, or businesses that while not normally cash intensive,**

generate substantial amounts of cash for certain transactions; Unregulated charities and other unregulated “not for profit” organisations (especially those operating on a “cross-border” basis); Dealers in high value or precious goods (for example, jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers); Accounts for “gatekeepers” such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution. Accounts for clients introduced by such gatekeepers may also be higher risk where the financial institution places unreasonable reliance for KYC and AML matters on the gatekeeper and the use or involvement of intermediaries within the relationship. Also included were customers that are **politically exposed persons or “PEPs”** were also included and financial services, particularly; **International Correspondent Banking** services, and **International Private Banking** services and services involving **Banknote and Precious Metal trading and delivery**.

According to the Wolfsberg Group, certain variables may increase or decrease the perceived risk posed by a particular customer or transaction and may include: (i) **the level of assets** to be deposited by the particular customer or **size of transactions undertaken**. For example, unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may mean that customers not otherwise seen as higher risk should be treated as such. Conversely, low levels of assets or low value transactions involving customers that would otherwise appear to be higher risk mean that a financial institution may decide to treat such customers as lower risk within an overall risk based approach; (ii) **the level of regulation or other oversight** or governance regime to which a customer is subjected. A customer that is a financial institution, for example, regulated in a jurisdiction recognised as having adequate Anti-Money Laundering (AML) standards (or is part of a group that implements a group standard where the parent is subject to adequate AML regulation and supervision and the parent of the customer exercises appropriate oversight over the customer) poses less risk from a money laundering perspective than a customer that is unregulated or subject only to minimal AML regulation; (iii) companies and their wholly owned subsidiaries that are **publicly owned and traded** on a recognised exchange pose minimal money laundering risks. Even though it may become substantially more difficult to distinguish between legitimate and illegitimate transactions, these companies are usually from jurisdictions with an adequate, recognised

regulatory scheme, and therefore, generally pose less risk due to the type of business they conduct and the wider governance regime to which they are subject. In addition, the necessity to have a specific understanding of each of the transactions conducted by these companies is mitigated by the nature of the company (publicly owned and traded from jurisdictions with adequate controls). Moreover, these entities may not need to be subjected to as stringent account opening due diligence or transaction monitoring during the course of the relationship; (iv) **regularity or duration of the relationship**: long standing relationships involving frequent client contact throughout the relationship may present less risk from a money laundering perspective; (v) **the familiarity with a jurisdiction**, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as the result of an institution’s own operations within the jurisdiction. Greater familiarity will enhance the ability of the institution to assess the client. Note: use by clients of intermediate corporate vehicles or other structures that have no clear commercial or other rationale or that unnecessarily increase the complexity or otherwise result in a lack of transparency for the financial institution. Such vehicles or structures will increase the risk unless the rationale is understood and the structure is sufficiently transparent to the institution.

Additional Sources

From elsewhere (including see Part 2), customers potentially of additional concern and/or worthy of note or possibly on watchlists to consider in the future to money laundering professionals may include, **Embassies, Sovereign Wealth Funds or other State Bodies or State Owned Enterprises**, particularly where country risks are significantly elevated; **Private Military Firms**; companies dealing successfully in Countries where again risks are significantly elevated and the particular industry is more exposed to in particular corruption risks (see Part 1, Section 1, Bribery and Corruption); **Founders of major public companies** where the company is still run and effectively controlled by a founder or founders family where there are concerns over governance and/or transparency; individual **insiders**, senior business leaders trading in their own or related stock ahead of announcements or during restricted periods or without adequate market disclosure; **hedge funds and/or hedge fund managers** including successfully profiting ahead of public announcements, or Funds producing too regular or too predictable positive results, suggesting possible fraud; **Import and export companies** involved in trading items regularly smuggled, for example alcohol or tobacco; and **carbon credit traders**.



Sub-section 2. Customer Risks

- Arms Dealers, 139
- Banks & other Financial Institutions, 141
- Cash-Intensive Businesses, 145
- Casinos including Internet Gambling, 145
- Charities & Not For Profit Organisations, 152
- Gatekeepers, 154
- High Value Goods Dealers, 157
- Intermediaries, 161
- Money Services Businesses, 162
- Politically Exposed Persons, 166
- Precious Metals & Stones Dealers, 169
- Private Military Firms, 173
- Real Estate Agents, 173

Arms Dealers

"You know who's going to inherit the world? Arms dealers. Because everyone else is too busy killing each other."
The character Yuri Orlov in the movie "Lord of War"

Introduction

The defence industry has undergone significant change following the end of the arms race and the Cold War. Defence production and weapons procurement are no longer the epicentre of foreign policy or defined as state assets. Military spend has reduced and the industry has globalised, accelerated in part by modernisation and the need for cutting edge technology. This has left a relatively small number of legitimate giant suppliers with transnational supply chains. Stockpiles of old Soviet weapons and arms related unemployment have also had an impact. It is estimated that for 2010 US\$1.735 trillion was spent annually on military expenditures worldwide.² This represents 2.5% of World 2011 GDP – a decrease from the 1990s when the figure was closer to 4%.

Whilst the industry has globalised and modernised over the past 20 years, the industry is prone to corruption. According to Transparency International, the defence industry is the most corruption-prone of all international businesses. In the US, it is estimated that the defence sector accounted for almost 50% of all bribery allegations in 2006. It is not surprising then, that many of today's leading global defence contractors such as Lockheed, BAE and Thales have been embroiled in some sort of corruption scandal. In the US, the widespread practice by defence contractors in the 1970s of bribing foreign government officials to win business, led directly to the enactment of the FCPA.

Corruption can in part be attributed to the heavy reliance placed by defence contractors on intermediaries who are handsomely rewarded and often engaged only because of their connections. Cases such as BAE, Bofors, Thomson CSF and Lockheed all involved complex webs of commission payments, offshore bank accounts and intermediaries. Middlemen such as Adnan Khashoggi attained notoriety for his role in arms deals and openly flaunted his wealth and close relationships with key decision makers.

Although a legitimate industry may have globalised, regulation and controls have not, leading to a highly profitable black market. Since the end of the Cold War, there has been a proliferation of opportunistic individuals involved in the arms business, particularly those in trafficking to Africa, creating a black market

estimated at US\$1bio a year.³ For more details see Part 1, Section 1, Illicit Arms Trafficking and Part 2, Section 7, Criminal Cases; Illicit Arms Traffickers; Mohamed al-Kassar, Viktor Bout, Tomislav Damjanovic, Pierre Falcone, Adnan Khashoggi, Simon Mann, Leonid Minin and Basil Zaharoff.

Definition/Description

Arms dealers are individuals or companies involved in the manufacture, provision, sale, purchase, distribution or hire of defence, arms or war related materials (arms, aircraft, ships, tanks, military equipment, weapons systems spares, ammunition explosives etc). Research and development, technology and electronic systems plus ongoing support and service are increasingly important products and services. There are a range of actors who might fall within this definition or be involved in transactions. For example, a large defence company such as global giants Lockheed or BAE Systems; a company or individual who acts as a facilitator, intermediary or other service provider on behalf of a contractor or end customer; an end customer (traditionally a government); or a government official or other PEP, who is in a position of influence (or closely associated with) with respect to defence spending, procurement and awarding contracts. Private military firms are considered in further detail in their own right later in this Sub-section 2.

The top ten countries with the highest defence budgets for 2010 are set out below.

Countries Top 10 Defence Budgets 2010			
Country	Spending US\$bio	World Share (%)	% of GDP 2011
1 US	711	41	4.7
2 China	143	8.2	2
3 Russia	71.9	4.1	3.9
4 UK	62.7	3.6	2.6
5 France	62.5	3.6	2.3
6 Japan	59.3	3.4	1
7 India	48.9	2.7	2.5
8 Saudi Arabia	48.5	2.8	8.7
9 Germany	46.7	2.7	1.3
10 Brazil	35.4	2	1.5
World Total	1735	74.3	2.5

Source: Stockholm Int Peace Research Institute 2011⁴

These Top 10 represent 74% of total world spending.

2010 Top 10 Arms Importers (US\$)	
Importer	US\$
1 India	3,33bio
2 Saudi Arabia	2,58bio
3 Australia	1,68bio
4 South Korea	1,13bio
5 Singapore	1,07bio
6 US	893mio
7 Algeria	791mio
8 Pakistan	787mio
9 Greece	703mio
10 China	559mio

Source: Stockholm Int Peace Research Institute 2011⁴

2010 Top 10 Arms Exporters (US\$)	
Country of Supplier	US\$
1 US	8,6bio
2 Russia	6bio
3 Germany	2,35bio
4 France	1,83bio
5 China	1,42bio
6 UK	1,05bio
7 Sweden	806mio
8 Italy	627mio
9 Spain	513mio
10 Netherlands	503mio

Source: Stockholm Int Peace Research Institute 2011⁵

Human Rights Groups and charitable organisations such as Oxfam campaign⁶ widely for the need to regulate the supply of arms and have complained that UN efforts to establish a global arms trade treaty have been unsuccessful due to opposition from countries which are major arms exporters. However, recently the UN passed an Arms Treaty, The Arms Trade Treaty 2013, which provides for common international standards for the import and export and transfer of conventional arms. Arms embargoes imposed by the UN though are regularly contravened with little enforcement action, let alone successful convictions. In Angola for example, the French Government assisted

the procurement of arms on behalf of the ruling party in direct contravention of the UN Embargo via Pierre Falcone and others.

Money Laundering/Terrorist Financing Risks

Conflict zones and instable political environments, where arms dealers often operate, have weak infrastructures, little or no accountability or rule of law, one party leadership and opposing rebel groups. Weapons once legally manufactured and traded may be later purchased in cash or countertraded for oil, diamonds or other commodities on the blackmarket. Leonid Minin, for example, supplied Liberian, President Charles Taylor, helping him commit genocide in neighbouring Sierra Leone. Tomislav Damjanovic and, of course, Victor Bout also traded arms with many others including Jonas Savimbi, the leader of the UNITA rebel group in Angola in exchange for diamonds. Arms dealers operating in the black market are also likely to be involved in or facilitate murder, drug trafficking and other organised crimes.

The market characteristics of the defence industry also make it easy for illegal trade to flourish. Traditionally, the industry has been highly concentrated, with a small number of customers (usually governments) who have a monopoly as sole purchaser. Power and decision making is further concentrated in a small number of individuals who are public officials or PEPs and therefore such agreements can pose Grand Corruption risks for example see Bofors; Lockheed Martin; BAE Systems and Thomson CSF-Thales. On the supply side, there are a relatively small number of manufacturers or contractors: contracts are usually long term (sometimes decades) with highly lucrative fees in the billions of dollars; offset arrangements are usually built in to contracts which are opaque and not clearly defined; and, there is a general lack of transparency around arms contracts, sales and commissions, usually on the proclaimed basis of national interest and state secrecy.

Cash flows involved are usually complex, making identification of the true originators and recipients sometimes impossible to establish. Flows of money are often channelled through multiple shell companies, into various offshore accounts and via numerous handling agents and nominee companies and via intermediaries. Examples of intermediaries, particularly of note, include Adnan Khashoggi and Pierre Falcone, but also Andrew Wang (see Thomson CSF-Thales). Legitimate businesses often pay secret commissions to offshore companies or agents without taking appropriate due diligence steps to identify the true purpose behind the payments. The obfuscation is of course often deliberate, such as was the case with BAE Systems and Thomson CSF-Thales.

Banks & other Financial Institutions

"Cause that's where the money is." Willy Sutton

Allegedly in response to the question, "Willie, why do you rob banks?" posed by a journalist, serial US Bank Robber Willie Sutton, also known as "Slick Willie", answered this phrase that is now considered an urban legend.

Introduction

Paradoxically, whilst the odd bank robbery is still carried out the proceeds of crime and the laundering of criminally derived funds are a much greater threat to a bank. Criminals use banks at each stage of the money laundering process, trying to disguise the criminal origin of the funds in the mass of other people's monies that Banks are responsible for looking after.

Definition/Description

FATF as per Recommendation 1 of their 40 AML/CTF Recommendations, expect all countries to require banks and other financial institutions, "to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks," and then through Recommendations 10-21 provide specific measures that apply to financial institutions.⁷ For details see Part 1, Section 3, Laws and Regulations, FATF below. The underlying rationale for these Recommendations is due to the fact that, as Willie Sutton ruefully supposedly replied, banks are where the money is. Additionally, banks operate as intermediaries between savers and borrowers, both individuals and businesses and also operate the global payment system; and as such are the fulcrum of the international financial system. For more details on the workings of the international payment system see Part 1, Section 2, Sub-section 3, Products and Services Risks; A Brief History of Banking and Correspondent Banking.

Banking in the modern sense of the word can be traced to medieval and early Renaissance Italy, to the rich cities in the north like Florence, Venice and Genoa. The Bardi and Peruzzi families dominated banking in 14th century Florence, establishing branches in many other parts of Europe. One of the most famous Italian banks was the Medici Bank, set up by Giovanni di Bicci de' Medici in 1397. The earliest known state deposit bank, Banco di San Giorgio (Bank of St. George), was founded in 1407 at Genoa, Italy. The oldest bank still in existence is Monte dei Paschi di Siena, headquartered in Siena, Italy, which has been operating continuously since 1472.

It is followed by Berenberg Bank of Hamburg (1590) and Sveriges Riksbank of Sweden (1668). The word bank was borrowed from "banque" in French, "banca" in Italian and "bank" in German which means bench or counter. Benches were used as desks or exchange counters during the Renaissance by Florentine bankers, who used to make their transactions atop desks covered by green tablecloths. The term bankrupt is a derivative and was used to denote the destruction of the counter and the end of business for a banker that had lost money and could no longer operate. For more details see Part 1, Section 2, Sub-section 3, Products and Services Risks and in particular "A History of Banking" below. The Worlds largest banks by assets size are:

Top 25 Banks by Assets (US\$ trillion)			
No	Name	Home	Assets
1	Ind & Com Bank of China	China	3.1
2	HSBC Holdings	UK	2.7
3	Credit Agricole Grp	France	2.6
4	BNP Paribas	France	2.5
5	Mitsubishi UFJ Fin Grp	Japan	2.5
6	JPMorgan Chase	US	2.5
7	China Construction Bank	China	2.5
8	Deutsche Bank	Ger	2.4
9	Agriculture Bank of China	China	2.4
10	Barclays PLC	UK	2.3
11	Bank of China	China	2.2
12	Bank of America	US	2.1
13	Japan Post Bank	Japan	2.1
14	Citigroup Inc	China	1.9
15	Mizuho Financial Grp	Japan	1.9
16	Royal Bank of Scotland	UK	1.8
17	SocGen	France	1.7
18	Banco Santander	Spain	1.6
19	Groupe BPCE	France	1.5
20	Sumitomo Mitsui Fin Grp	Japan	1.5
21	ING Grp	N'land	1.5
22	Wells Fargo	US	1.5
23	Lloyds Banking Grp	UK	1.4
24	China Development Bank	China	1.2
25	UBS	CH	1.2
Total			50.6
Source: www.relbanks.com - Setember 2013			

There are more than 10,000 banks that use the SWIFT international payment network, representing 212 countries.

The US has the most banks in the world in terms of institutions 7,085 (at the end of 2008) with Germany in second place with 2,400 (at the end of 2006 according to the Centre for Economic Research) and Russia in third place with 1,200 (at the end of 2006 according to the Centre for Economic Research).

No other country in the world has more than 1,000 banks, for example Japan had 129 banks (at the end of 2008). Assets of the largest 1,000 banks in the world were US\$96.4 trillion in the 2008/2009 financial year with profits of US\$115bio.

EU banks held the largest share of the total, 56% in 2008/2009, Asian banks 14% and US banks 13%. Assets of the largest 500, were US\$62mio and of the largest 25, Fee revenue generated by the top ten global investment banking totaled US\$72.1bio in 2011.

Banks' activities can be divided into retail banking, dealing directly with individuals and small businesses; commercial banking, providing services to mid-market business; corporate banking, directed at large business entities; private banking, providing wealth management services to high net worth individuals and families; correspondent banking, providing banking services to other banks; and investment banking, relating to activities in the financial markets. Banks are also acting as credit card companies or issuers and brokerages providing access to the financial markets, including securities such as equities. For more details see Part 1, Section 2, Sub-section 3, Products & Services Risks below.

Banks offer many different channels to access their banking and other services including by automated teller machines, in retail branches, call centres and telephone banking; by mail: most banks accept cheque deposits via mail and use mail to communicate to their customers, for example, by sending out statements; by mobile banking, by using a mobile phone to conduct banking transactions; by video banking, by performing multiple transactions, payments etc. over the internet; by relationship managers, mostly for private banking or business banking, often visiting customers at their homes or businesses; banking used for performing banking transactions or professional banking consultations via a remote video and audio connection.

Money Laundering / Terrorist Financing Risks

Banks and other financial institutions have been and continue to be targeted by criminals, money launderers, terrorists and terrorist financiers in many ways. The services that banks and other financial institutions offer can be abused by these people, exploiting the vulnerabilities of some products and services, and seeking to disguise themselves and their actions alongside millions of other legitimate transactions. In particular, inherent vulnerabilities and or attractiveness to criminals in wealth management/private banking and correspondent banking are probably the most obvious, though other products and services have also been abused too, including banknotes trading, precious metals dealing, trading, securities brokerage, credit cards, retail and commercial. In fact there is probably no area of banking that has or does not suffer from targeted abuse from criminals and their funds.

For a comparison of the inherent risks presented through the offering of banking products and services, see Part 1, Section 2, Sub-section 3, Products and Services Risks and in particular in Risk Assessment in Part 1, Section 4 below.

Sometimes criminals will come from the ranks of the bank's own staff, in the form of rogue trading, employee fraud, or corruption, or be working with or for external criminal gangs, though this is thankfully rare, banks are known to be targeted and their impact can be devastating.

Banks posing the greatest inherent risk are those with significant customer, country, product and services and channels risk exposures. These banks may still not be considered high risk provided they have designed and implemented effective comprehensive Money Laundering Prevention Programmes as they are required to do.

For more details see Part 1, Section 4, Money Laundering Prevention Programmes for details.

Additionally a number of banks, bank types and bank products and services have been highlighted as posing very high risks and these should be identified and appropriate action taken. For example, banks in countries where FATF has recommended counter-measures be applied, banks sanctioned or designated by relevant authorities and so called shell banks.

Cash Intensive Businesses

"Organised Crime in America takes in over US\$40bio a year and spends very little on office supplies"

Woody Allen, Comedian

Introduction

With cash being generated by many profitable crimes, such as drug trafficking, counterfeit and piracy, smuggling, human trafficking and illegal gambling, businesses are used as a cover in order to launder these criminal proceeds. Businesses that are particularly established or taken over are those that are cash based anyway, such that the taking and deposit of large amounts of cash into a business bank account is not unusual. As such cash intensive businesses can provide a cover for depositing additional, illegally earned cash into a bank account, and the payment of suppliers, both domestically and internationally, provides a good excuse for transfers of amounts of all sizes.

For some the term money laundering was coined to describe the actions of US mobsters during 1920s and early 1930s era of Prohibition. Their activities, which included sale of alcohol, illegal gambling and prostitution, generated large amounts of physical cash, much of which was in coins, so they owned and operated both slot machine and laundromat businesses, both of which took coins to operate the machines, and the coins could therefore be deposited without suspicion into front company bank accounts appearing legitimate. For more details see 'What is Money Laundering' in Part 1.

Cash intensive businesses may also be used to facilitate money transfers acting as an intermediary between sender and recipient, in much the same was as a money transfer business, with the potential for underground banking taking place and the potential vulnerability of facilitating terrorist finance either unwittingly or unwittingly.

Definition/Description

According to the BSA Exam Manual, "cash-intensive businesses and entities cover various industry sectors. Most of these businesses are conducting legitimate business; however, some aspects of these businesses may be susceptible to money laundering or terrorist financing. Common examples of cash-intensive businesses: convenience stores; restaurants; retail stores; liquor stores; cigarette distributors; privately owned automated teller machines (ATM); vending machine

operators and parking garages. The US BSA Exam Manual also highlights risks with those involved in bulk shipments of cash. According to UK Guidance, (JMLSG) the focus is on high cash turnover businesses, they include: casinos, bars, clubs, taxi firms, launderettes and takeaway restaurants.

Money Laundering/Terrorist Financing Risks

Whilst cash remains significant as a mode of payment for criminal products and services, the need to launder that cash will require the establishment or takeover of cash-intensive businesses.

Retail Type Outlets

Examples are numerous, but include The Pizza Connection, where Al Dente's Pizzeria in New York, was used by the Italian American Mafia, to launder drug trafficking proceeds, jewellers identified in the La Mina/Operation Polar Cap case and Speed Joyeros, who laundered for Colombian drug traffickers and Carnival French Ice Cream, which operated as an unlicensed money transfer business in New York via an Ice Cream Parlour. It is perfectly legitimate and understandable why many businesses operate mainly in cash, or take cash regularly. In many parts of the world, cash is still the dominant medium of exchange and even in many highly industrialised countries, many people do not have credit or debit cards. Nevertheless, where cards are readily available, the traditional benefits of accepting cash are diminishing, though good reasons remain. For example, with cash, the business receives payment immediately, with no waiting for a cheque to process or a card transaction to show up in the businesses account, avoiding concerns about fraud, bounced cheques or bogus credit/debit cards. Also there are no fees for card payments, which can reduce profit on each business transaction, particularly an issue when the transaction is small.

When establishing and maintaining banking relationships with these cash-intensive businesses, whilst most will be simple and straightforward and operate legitimately, there may be exceptional cases where there is an increased need to understand the customer's business operations; the intended use of the account; including anticipated transaction volume, products and services used; and the geographic locations involved in the relationship. In particular areas of increased risk may include factors or more likely a combination of factors which could include: the KYC information available and updated; the volume, frequency, and nature of cash and cash related transactions; the use of products and services and the Geographic footprint of the business, its customers and suppliers. For example, whilst documentary evidence may have been collected as to the

business owner, is the owner personally known, a long standing customer and/or the owner of a business that has been visited by the bank. A cash-intensive business that purports to be successful may, upon visiting the premises be obviously bogus, if the business is, for example, run-down or empty of customers, particularly at busy times. A business that has a high cash turnover may stand out versus equivalent businesses especially in that area or region so comparing businesses that can be clustered and identifying those that stand out may also be useful. For example, in the case of Carnival French Ice Cream, an ice cream parlor in New York City, filed approximately US\$185,000 which were the receipts from the legitimate business. Nevertheless, during the period 1996-2003 the business also acted as an illegal money transmitter, making payments to the Middle East and in particular Yemen of almost US\$22mio. Payments were also made to Saudi Arabia, UAE, Thailand, Canada and China which were unlikely to appear to have anything to do with the ice cream business.

Another risk area to consider is the use of other products and services. Illicit cash-intensive businesses are probably less likely to apply for credit, utilise non-face-to-face business channels to communicate and transact and are well aware of bank reporting thresholds and so avoid triggering these.

As a result for those customers deemed to be particularly higher risk, banks should consider additional periodic on-site visits, interviews with the businesses' management, and/or closer reviews of transactional activity and product and service usage. Most cash-intensive businesses, the use of cash registers or POS (point-of-sale) machines to record sales is common place, so cash sales should still be recorded and the use of invoices and other paperwork can also substantiate a cash transaction. Where necessary this additional substantiation of a customers business activities could be requested, along with tax filings and the like.

Private Automated Teller Machines (ATMs)

Whilst bank owned ATM machines have become ubiquitous, the growth in private owned ATMs also known as "white label" cash machines in many countries, now outnumber those owned and offered by Banks, being a lucrative industry, placed in hotel lobbies, bars and food courts, they provide quick access to cash, albeit with a hefty charge, either owned by the retailer or by private non-bank businesses such as Independent Sales Organisations (ISO). Although all privately owned ATMs are not high-risk, they are particularly susceptible to money laundering and fraud related activities.

A Report from Canada by the Canadian Police, the RCMP, claims that the Hells Angels biker gang control at least 5% of the private ATM business in Canada, with at least C\$315mio a year possibly being laundered through these white-label ATMs. For example, the Hells Angels are suspected of arranging to have an ATM placed in a club. The owner of the club, a front person chosen for their lack of criminal record, would apply for the necessary security clearance and, after receiving it, could stock the machine with a mix of bar proceeds and criminal drug proceeds. As long as the machine stayed under a safe limit, say C\$5,000 a day, it would be unlikely to draw attention.

Key to risk mitigation is effective KYC, on the owner if a private retail owned ATM or on the ISO, for example, obtaining information from the ISO regarding due diligence on its sub-ISO arrangements, such as the number and location of the ATMs, transaction volume, currency volume, and evidence regarding the source of any replenishment currency, for example evidence as to the sources of currency for the ATMs by obtaining copies of armored car contracts or lending arrangements. In addition scrutiny of transaction activity to identify excessive unusual usage and reviewing expected ATM activity levels, including currency withdrawals.

Bulk Cash Shipments

Bulk shipments of cash are made legitimately by land, sea and air. Those involved may be individuals or businesses that generate currency from cash sales of commodities or other products or services (including monetary instruments or exchanges of currency). Shippers also may be "intermediaries" that ship currency gathered from their customers or other intermediaries, normally banks, central banks, non-deposit financial institutions, or agents of these entities. Still as cash smuggling is one of the major mechanisms used by organised criminal gangs to move illicit funds out of countries, those that receive the smuggled bulk cash must find ways to re-integrate the currency from where it comes. Bulk shipments of currency come from shippers, usually Bank's that are presumed to be reputable but the cash may nevertheless originate from illicit activity. The monetary proceeds of criminal activities, for example, often reappear in the financial system as seemingly legitimate funds that have been placed and finally integrated by flowing through numerous intermediaries and layered transactions that disguise the origin of the funds. Layering can include shipments to or through other jurisdictions.

Casinos Including Internet Gambling

"For every dollar of revenue generated by gambling taxpayers must pay at least three dollars in increased criminal justice costs, social welfare expenses, high regulatory costs and increased expenditures."⁹

John W Kindt, Professor of Bus Admin, University of Illinois

Additional quotes from John Kindt include:
"Although crime and corruption decreases within a one mile radius of a casino, it increases 10% within a 35 mile radius by the third year the casino is open".

"The ABCs of legalised gambling - addictions, bankruptcies and crime".

"Gamblers spend 10% less on food, 25% less on clothing and 35% less on savings".

"Every slot machine takes US\$60,000 out of the local economy".

Introduction

Gambling in one form or another is as old as recorded history, though it has never been as popular as it is today. According to FATF,⁹ statistics from 2007 show that over 150 countries participate in some kind of legal gambling and 100 of these countries have legalised casinos. Over 100 countries offer some kind of lottery product and over 60 countries participate in the racing and sports betting industry.

Whilst the size of the gambling market conducted through legalised casinos was approximately US\$100bio in 2009 according to PWC,¹⁰ casinos despite regulation, are high-volume cash businesses and Casinos are still susceptible to money laundering.

Of even greater concern are illegal gambling operations which exist outside of the formal regulated sector and internet gambling sites. The illegal gambling market is estimated by Havocscope at US\$140bio.¹¹

Whilst the US has been the world's largest casino gaming market, this is set to change in 2013 according to PWC who predict that Asia will take over the number one spot.

Major Casino Markets by Revenues		
1	US	US\$57bio
2	Asia	US\$21bio
3	EMEA	US\$17bio
4	Canada	US\$3bio
5	LATAM	US\$425mio
	TOTAL	US\$100bio

Source: PWC 2009

More recent figures from PWC in 2011, give Asia revenue of US\$34.3bio and expected to grow to US\$79.3bio by 2015. For Canada, PWC report for 2010 an increase to US\$5.7bio and for Latam an increase to US\$3.8bio.

Major Casino Locations		
1	Macau	US\$15bio
2	Las Vegas, US	US\$10bio
3	Singapore	US\$2bio
4	France (including Monaco)	US\$4bio
5	Atlantic City, US	US\$4bio
6	Australia	US\$2.6bio
7	South Korea	US\$2.4bio
8	Germany	US\$2bio
9	South Africa	US\$1.6bio
10	UK	US\$1.2bio
11	Poland	US\$1.1bio
12	Niagara Falls, Canada	US\$1.1bio

Source: PWC 2009

Asia is no stranger of course to gambling. The Chinese recorded the first official account of the practice in 2300 BC, but it is generally believed that gambling in some form or another has been seen in almost every society in history. From the ancient Greeks and Romans to Napoleon's France and Elizabethan England, much of history is filled with stories of entertainment based on games of chance. The first known European gambling house, not called a casino although meeting the modern definition, was the Ridotto, established in Venice, Italy in 1638 to provide controlled gambling during the carnival season. It was closed in 1770 as the city government perceived it to impoverish the local gentry. In American history, early gambling establishments were known as saloons. The creation and importance of saloons was greatly influenced by four major cities; New

Orleans, St. Louis, Chicago and San Francisco. It was in the saloons that travellers could find people to talk to, drink with, and often gamble with. During the early 20th century in America, gambling became outlawed and banned by state legislation and social reformers of the time.

However, in 1931, gambling was legalised throughout the state of Nevada, along with Las Vegas and Reno. America's first legalised casinos were set up in those places. In 1978 New Jersey allowed gambling in Atlantic City, now America's second largest gambling city.

As high-volume cash businesses, casinos were the ideal businesses to be owned, controlled or used by money launderers, particularly organised crime and taking advantage of the change in the law in Nevada that legalized gambling, the *Italian American Mafia* via one of its most colorful lieutenants, Benjamin "Bugsy" Siegel. Before Bugsy focused on Las Vegas, Las Vegas was nothing more than a desert town inhabited by cowboys and a few slot machines. After Bugsy and fueled by Mob money, Las Vegas grew and grew. Before Las Vegas, American tourists looking for a good time had to travel all the way to Cuba, so Las Vegas was much closer to home and only a little over a decade after the first casino opened in Las Vegas, Fidel Castro's Cuban Revolution led to the closure of the Cuban Casinos.

Monaco is also a longstanding, well known location for casinos and gambling.⁷

Definition/Description

FATF have identified a class of businesses they call, "Designated Non-Financial Professions and Businesses (DNFPBs)" being professions and businesses that are seen as being attractive to money launderers and these are: casinos, (when their customers engage in financial transactions above US\$/€3,000), lawyers, accountants and trust and company service providers, dealers in precious metals and stones (when their customers engage in cash transactions above US\$/€15,000) and real estate agents. Casinos are the only form of gaming or gambling explicitly covered by the FATF standards however the FATF standards do not define casino or gaming, nor do they set out the activities undertaken by casinos. Casinos were the first non-bank financial institutions required to develop AML compliance programmes.

In addition to gaming, casinos offer a variety of financial services including accounts, credit, funds transfers, cheque cashing, and currency exchange often operating 24 hours a day with high volumes of cash transactions

taking pace very quickly.

The term "casino" is of Italian origin, the root word being "casa" (house) and originally meant a small country villa, summerhouse or pavilion. The word changed to refer to a building built for pleasure, usually on the grounds of a larger Italian villa or palazzo. Such buildings were used to host civic town functions – including dancing, music and gambling. In modern day Italian, this term designates a bordello (also called "casa chiusa", literally "closed house"), while the gambling house is spelled casinò with an accent. During the 19th century, the term "casino" came to include other public buildings where pleasurable activities, including gambling, and sports took place.

Casinos usually involve customers gambling by playing games of chance, in some cases with an element of skill, such as roulette and craps, card games such as blackjack and poker and of course lottery, fruit or slot machines. Casinos may also provide facilities to place bets on sports, traditionally on horses but now more generally across various sports and not just on the result. Most games played have mathematically-determined odds that ensure the Casino has at all times an advantage over the players, known as the house edge. In games such as poker where players play against each other, the house takes a commission called the rake. Casinos sometimes give out complimentary items to gamblers.

Money Laundering/Terrorist Financing Costs

Casinos have long been recognised as vulnerable to money laundering abuse, largely due to the volume of cash involved and through the process of gambling, proceeds of crime can become effectively laundered into legitimately acquired funds, albeit likely at a cost. As casinos also provide services similar to those provided by financial institutions, including accounts, credit, funds transfers, cheque cashing, and currency exchange, they face similar risks to financial institutions.

Today casinos are in many parts of the world highly regulated but in others regulation is developing, patchy and in some effectively non-existent. Even in well regulated jurisdictions, casinos report high incidences of money laundering.

Money laundering schemes involving casinos usually start with the purchase of casino chips using illicit cash. The chips then can be used in the following ways. After de minimis gambling, chips are: i) cashed in for a casino cheque or wire transfer that is deposited

into a bank account, ii) used as a form of currency for goods and services, particularly illegal narcotics, so that others ultimately cash in the chips; and iii) used for gambling to generate certifiable winnings.

Whilst criminals will structure transactions at banks and MSBs to avoid transaction records or reports that draw attention to them, they use casinos for the opposite purpose. Having a CTR filed on a casino payout has the effect of making the money appear legitimate. Criminals also use casinos to launder counterfeit money, as well as large currency notes that would be conspicuous and difficult to use elsewhere. For example, Australia's hotel poker/slot machines are increasingly being used by criminals to launder millions of dollars each week. Criminals deposit A\$10,000 at a time and once a few bets have been made cash out and collect a casino cheque for the portion of the remaining funds. The trick is so well known to criminals that the hotels offering poker machines are referred to as "LLs" - Local Laundries.

Of particular concern outside of well regulated jurisdictions and casinos, are those experiencing significant growth, poorly regulated jurisdictions, particularly those located in geographic areas characterised by poor governance, political instability or bordering regions with significant crime or terrorist problems. Additional concern areas include illegal casinos and gambling houses, high seas casinos, junkets, and VIP rooms and internet gambling.

Whilst it is conceivable that casinos could be used in connection with terrorist financing there are no reported examples, and any such activity would look like possible money laundering and not terrorism finance in any event.

Significant Growth and Emerging Markets

Singapore is significantly expanding as is Papua New Guinea. Macau continues to grow, with a new push since 2004 when the opening of the Sands Macau ushered in a new era of American brands opening in the Chinese enclave. In the US, tribal casinos have moved rapidly from relative obscurity within the US casino industry to a position of prominence in the past 15 years. Tribal casinos now surpass Nevada revenue by more than two-fold.

Significant activity in emerging markets can be seen in Asia and Africa. A number of developing countries with cash based economies and weak AML frameworks are looking at casinos including Palau and East Timor. The poor regulation or existence of casinos in countries with weak AML regimes are attractive venues for criminals,

particularly organised crime groups who seek to control or own casinos or aspects of casino operations. Criminals attempt to infiltrate or influence casinos to facilitate theft, fraud, money laundering, loan sharking and other crimes. Loan sharking is prevalent in casinos in a number of jurisdictions and indeed many junket operators (see Junkets below) extend credit as part of their service package. It is believed that organised crime groups work with the junket operators to extend "credit" at rates beyond any legal maximum to gamblers. Persons in debt to loan sharks are then vulnerable to coercion strategies to assist money laundering schemes in casinos.

Illegal Casinos and Gambling

Illegal casinos and gambling generate more than the total revenue from the formal regulated sector at over US\$140bio a year. Not surprisingly the involvement of organised crime is prevalent. From the early days in Las Vegas the *Italian American Mafia* and in Asia with Chinese organised crime gangs such as the Triads operate to either control or use casinos, both legal and illegal as appropriate to generate and launder criminal proceeds. One of the countries where illegal gambling is particularly prevalent is Thailand. Following a detailed study by the Thai Government it was revealed that there were between 200-300 illegal casinos or gambling houses in Bangkok with up to US\$17bio generated through illegal gambling in the country both in the cities and close to the border, particularly with Myanmar. Whilst Thailand has tried to tackle the problem, including by arresting over 100,000 people a year, illegal gambling shows no sign of being curtailed. The business is fuelled by Thai junket operators offering and providing casino tourism services to mostly Asians, particularly Chinese, providing transportation accommodation and moving money from for example China to Thailand and providing local or foreign currency in which to play. As many of the illegal casinos and gambling houses are located close to borders and/or require movements of people and monies across borders, it is thought that, especially where organised crime is involved that networks and connections with smuggling, human and drug trafficking are made.

High Seas Casinos

High seas gambling (also called boat gambling or floating casinos) involves gaming vessels that travel to international waters to conduct gaming/casino activities. These may be long-distance cruises that have gaming/casinos as side entertainment, or short distance trips that are directed solely at gaming. Gambling on the high seas boasts many attractions. For one, with rare exception it is tax-free and out of government supervision. The prevalence of gambling in international waters is an

issue for all countries with cruise ships registered or operating within their jurisdiction. While many countries prohibit casinos on ships from operating in territorial waters, cruise ship gambling in international waters is not well regulated.

Few jurisdictions have regulatory oversight over cruise ship casinos registered to their jurisdiction and fewer have AML/CFT controls over cruise ship casinos. Since cruise ship casinos, with only minor exceptions, are allowed to operate only when in international waters the casinos are largely unregulated. Whilst some steps have been taken within the cruise line sector to self regulate via the International Council of Cruise Lines (ICCL), it is unknown what general record-keeping or due diligence processes, if any, are carried out by cruise lines or if they report suspicious activities to appropriate authorities.

There are not many studies about the level of risk presented by gambling that is undertaken in international waters. For example, it is not readily apparent what methods are used to transfer funds to and from the cruise ship and any associated money laundering risks.

Regulatory control over "high seas gambling" raises complex questions of international law. If AML/CFT laws were to apply, it is not clear which jurisdictions would have oversight; the jurisdiction from which the ship is operating from, or the jurisdiction where the vessel is registered.

Some jurisdictions impose tax and AML regulations on cruise ship lines, such as the US. Ships registered in the US are subject to income tax and money laundering legislations, meaning that US citizens and permanent residents must declare any income from cruise-ship gambling with customs on returning to the US and through yearly tax returns. The cruise line is also required to file tax notices for jackpots of over US\$1,200. However, there is some question as to whether all US registered ships comply with these requirements, and it is unknown the nature or level of oversight by US authorities.

High seas gambling is an issue for many jurisdictions, for example Hong Kong where a number of cruise ships or large luxury vessels, operate from their harbours, with the sole or primary purpose of providing casino gaming in international waters. These vessels sail under foreign flags, so port jurisdictions have difficulty in imposing AML/CFT controls on these "foreign" vessels due to the limitation of extra-territorial jurisdiction. In very few cases do the AML/CFT rules of the "flag flying"

jurisdiction apply to the high-seas casino. The lack of supervision of casinos operating in international waters leaves port jurisdictions exposed to casino related money laundering risks.

Jurisdictions have raised the challenges faced by the issue of extra-territorial jurisdiction over gambling activities beyond flag-flying vessels, as per the current status of international law. There appears to be a need for further consideration of the issue and possible multilateral solutions.

Government bans on police officers patronising casinos further exacerbates the lawless culture on board a gambling boat. The Chinese Government has banned officials from gambling and tightened policies on tours to Macao, making casinos on the high seas even more popular. Government officials have frequented high sea casinos since the 1990s. One of the most infamous gamblers, Ma Xiangdong, former Vice Mayor of Shenyang City, visited Macao casinos 17 times and the Oriental Princess casino four times. He once allegedly lost tens of millions yuan within three days.

In 2008, mainland Chinese authorities arrested Lian Chao, nicknamed "Gambling King of the High Seas," for alleged money laundering for Huang Guangyu, the founder of home appliances chain Gome.¹³ Huang was taken into custody in late December 2008. Lian, one of the investors behind the Neptune fleet of casinos, often invited Chinese officials and businessmen aboard to gamble. Huang was one of his clients, and Lian is alleged to have helped him launder money through gambling. The Neptune is a five-star luxury ship in Hong Kong, nine stories tall, and with a capacity to accommodate 500 people.

Junkets

The largest money laundering loophole in certain jurisdictions is the fact that the AML regulation applicable to casinos may not cover "junket" operators. A junket is an organised gaming tour for people who travel to the casino primarily to gamble. The term Junket has its origins in Chinese where Jin literally means introducing and Ke means customers. It is a method of casino marketing developed in the late 1930s for introducing customers to the expanding Macau gaming industry. The junket may include transport, accommodation, incentives to play at the casino and the movement of funds to and from the casino. The junket may be run by the casino itself or an independent operator. Junkets appear to be common in casino jurisdictions in the Americas, Caribbean and Asia, but are less common in European Casinos. Operators of junkets account for more than half of Macau's gaming

revenue. As of January 2009, Macau had 153 licensed junket operators.

Junkets are also a convenient way for China's mainlanders to evade China's strict capital control requirements. Chinese law forbids its citizens from taking more than 20,000 renminbi (£1,800) over the border so wealthy mainlanders deposit their money with junket operators. China also has an annual cap of US\$50,000 on conversion of RMB to foreign currency further incentivising junket use.¹⁴ Once in Macau, the junkets dispense the money back to individuals, and extend credit, often two to three times the amount originally deposited with them. They bring the VIPs to the Casinos, and are paid huge commissions. Back on the mainland, gamblers who fail to pay up face menacing debt collectors. The other rather less acknowledged factor is money laundering. The junkets take in Chinese Renminbi (which cannot be converted on the world's money exchanges) while the casinos can pay out in dollars. Suitcases of dollars take the quick trip from Macau to Hong Kong, much of it pouring into the city's property market. Even bigger sums are believed to head into offshore tax havens. Whilst AML laws require application of KYC regulations to casino customers, the junket operators are able to circumvent this requirement by acting as an agent between the gambler and the casino. The junket operators have the ability to move large amounts of money across borders and through multiple casinos on behalf of their clientele and may use wire transfers to move funds on behalf of their clients. The identity of the junket client may be unknown to the sending and receiving financial institution or the receiving casino.

Relatively few casino jurisdictions regulate junkets. Whilst the US has a long history of regulating junkets, Macau has only recently taken steps toward clear regulation. Macau's efforts to strengthen enforcement in this area are evident. The Macau Public Prosecutions Office announced in October 2011 that the number of criminal cases handled by the office had increased 10% between January to August of 2011.¹⁵ The Office highlighted a growth in the number of AML cases connected with the gaming industry, mainly with illegal gambling in VIP rooms.

Whilst this enhanced enforcement is important, the Office should also focus on legal gambling in VIP rooms where authorised junket operators facilitate money laundering by allowing gamblers to shield their identity and hide behind the junket operator. The pressure for law enforcement to turn a blind eye cannot be overlooked. The Casinos are a huge cash cow for the Chinese state, too, which levies tax at 39% and, as

noted above, Hong Kong benefits from inflows from Macau.

VIP Rooms

Every casino in every gaming jurisdiction in the world has to deal with both substantial players ("VIP players") and regular players ("mass market customers"). The approach that Macau has taken is significantly different from the rest of the world. These two categories of players are ushered into two different casino systems and so make Macau's traditional casino industry a dual system, a VIP system and a "mass market" system.

The operational style of the mass market system of Macau's traditional casino industry is similar to what one would find in Nevada casinos. The unique part in Macau has been the VIP system. Macau's VIP-room contractual system began in the 1930s, and slowly evolved due to the special cultural and geographic conditions affecting Macau and southern China, and matured by the mid-1980s. Since the mid-1980s, Macau's casino industry has been dominated by the VIP sector; in terms of gross gaming revenues, VIP rooms captured about 70% of market share in 2004.

The VIP Room "contractual system" means the casino contracts with a VIP Room operator or promoter to operate a VIP Room at the casino.¹⁶ The VIP promoter enters into a contract with the casino company that outlines the rights and responsibilities of both parties. The documents are worded on room-by-room basis. The agreement usually sets out minimum dead chip sales (see below), rewards for over-selling, revenue sharing agreements and deposits promoters must pay.

The VIP promoter plays a pivotal role within the VIP-room system between the casino and junket operators. He is the organiser and maintainer of the interpersonal web of junket operators. He also serves as a lender to junket operators and occasionally to customers. The VIP promoter is also the one who bears major risk in terms of credit transactions within the VIP-room contractual system. VIP promoters can either be natural persons or legal persons. Whereas, a junket operator is typically a self-employed person who earns dead-chip commissions by selling his customers to a VIP promoter.

There are three major elements that construct the VIP room system: Dead Chips, VIP Rooms, and VIP Room Contracts. The dead chip, also called junket chip, non-negotiable chip, or clay chip, is a kind of casino chip which is sold or lent by the casino to VIP promoters or junket operators for betting purposes only. Dead chips are not cashable or refundable by customers, but are only usable in making wagers in the VIP room where

they were purchased or borrowed. Since the dead chip is financially less flexible, logically its price should be cheaper than regular casino chips. The dead chip's normal price is discounted by a certain percentage but face value remain the same. The difference is known as "dead chip commission" and functions as a payment vehicle for the casino to reward the marketing efforts of VIP promoters and junket operators. Customers cannot purchase or borrow dead chips directly from VIP room casino cages. The casino only sells or lends dead chips to VIP promoters and junket operators. VIP promoters and junket operators can only buy or borrow dead chips from the VIP room's cage, and VIP customers can only buy or borrow dead chips from VIP promoters or junket operators. Dead chips designed to guarantee the chips will actually be wagered on the gaming tables in that VIP room rather than going back to be cashed out at the cage without having been put into action. The customer is assured complete confidentiality via this arrangement.

The VIP room itself is an individual room or set of rooms within a larger casino specifically designed and designated for VIP customers' usage only. All properties of the VIP room still belong to the casino; the dealers and the gaming managers are employees of the casino; and the gaming operations of a VIP room are run by the casino. Often there are no documented contracts between VIP promoters and junket operators, whose cooperation and transactions are based on convention and oral agreements or, sometimes, simple bookkeeping. Furthermore, there was as of 2006 no regulatory requirement for the VIP contracts to be reviewed by regulatory authorities. If a VIP promoter is unable to meet his minimum sales in a particular period, then other VIP promoters who have exceeded their targets may shift some of their sales to help them out or, more commonly, the VIP operator "loans" the room to VIP promoters who have no contractual relationship with the casino. There is a general lack of transparency in who ultimately controls the VIP rooms behind the public face on the contract. VIP Rooms are widely known to be the domain of organised crime also offering loan sharking and prostitution services on top of anonymous gambling to the VIPs.

As more casinos operate in Macau, the competition for VIP customers increases causing profit margins to quickly get squeezed. Additionally, the casinos offering contracts to VIP Room operators do not play on a level playing field. Most of the new entrants into the Macau market that have significant casino operations in other jurisdictions - the American gaming companies Las Vegas Sands, Wynn Resorts, and MGM and the Australian company PBL - must adhere to stricter

standards than the Macau-owned casinos with respect to business practices of VIP promoters and junket operators. Therefore there will be ongoing competitive pressures to modify or change the VIP system in ways that are more compatible with their business models and regulatory sensitivities. After winning one of the original concessions, Wynn Resorts refused to break ground on its Macau casino until the legislation was changed that would allow the casino itself to grant credit, rather than being dependent on VIP promoters and junket operators for such services. An important consideration for this demand was the concern of being at the mercy of these independent contractors - many of whom might not be licensable by international regulatory standards - rather than agents employed directly by the casino for this important segment of the market.

Internet Gambling

Before the 1990s, individuals who wanted to place a casino or sports-type bet in the US basically had two choices: they could travel to a legitimate brick-and-mortar gaming establishment or place an illegal wager through a bookmaker. However, with the emergence of the internet in the mid-1990s, a new form of gambling appeared - on-line gaming casinos and sports wagering. Internet gambling involves any activity that takes place via the internet and that includes placing a bet or wager. Courts generally have defined a bet or wager as any activity that involves a prize, consideration, and chance. A prize is anything of value. Chance is usually determined by assessing whether chance or skill predominates. Consideration is what the person must pay to enter and must be something of value, such as money.

The first online gambling began in 1994 when Antigua and Barbuda passed the Free Trade & Processing Act, allowing gaming licenses to be granted to organisations applying to open online casinos. Online casinos would not have been possible without the development of gambling software paired with online security software to allow for secure transactions over the internet.

In 1996 the first regulation for online gaming activity came about through the establishment of the Kahnawake Gaming Commission (KGC).¹⁷ KGC regulates online gaming activity from the Mohawk Territory of Kahnawake and issues gaming licenses to many of the world's online casinos and poker rooms. This is an attempt to keep the operations of licensed online gambling organisations fair and transparent.

Internet gambling is a growing industry. During 1997 and 1998, online gambling gained popularity. Internet gambling websites increased from just 15 websites

in 1996, to 200 websites in 1997.¹⁸ According to a 2002 US GAO report,¹⁹ internet gambling operators established approximately 1,800 e-gaming websites in locations outside the US, and global revenues from Internet gaming in 2003 were projected to be US\$5bio. In 2008, H2 Gambling Capital estimates worldwide online gambling revenue at US\$21bio. Internet gambling has become one of the most popular and lucrative business present on the internet.

Efforts to control internet gambling did not meet with early success. In 1999, the US introduced the Internet Gambling Prohibition Act proposing to prohibit a company from offering any online gambling product to any US citizen but it did not pass. Multiplayer online gambling was also introduced in 1999. This was the first time people could gamble, chat and interact with each other in an interactive environment. US legislation finally succeeded in 2006 when the US Congress enacted the Unlawful Internet Gambling Enforcement Act ("UIGEA"), making it a crime to "knowingly accept" most forms of payment "in connection with the participation of another person in unlawful Internet gambling."

Whilst largely legal in most countries, multiple countries around the world have also taken legislative action to control internet gambling. In 2000, the Australian Federal Government passed the Interactive Gambling Moratorium Act,²⁰ making it illegal for any online casino not licensed and operating before May 2000 to operate. The new legislation meant Lasseter's Online became the only online casino able to legally operate in Australia; however, they cannot take bets from Australian citizens. India, France, Israel, Russia, and the UK, amongst others, have laws in place to control the downsides of this exploding industry.

Gambling money online can come from credit card, electronic cheque, certified cheque, money order, or even wire transfer. Normally, gamblers upload funds to the online gambling company, make bets or play the games that it offers, and then cash out any winnings. Gamblers can often fund gambling accounts by credit card or debit card, and cash out winnings directly back to the card. Due to the UIGEA most US banks, however, prohibit the use of their cards for the purpose of internet gambling, and attempts by Americans to use credit cards at internet gambling sites are usually rejected. A number of electronic money services offer accounts with which online gambling can be funded, however, many top fund-transfer sites have discontinued service for US residents. Payment by cheque and wire transfer is also common. Some gambling methods accept Bitcoin, a digital currency.

According to FATF, internet casinos are proving an attractive bet for criminals needing to launder their ill-gotten gains because of the difficulties encountered by the authorities in tracking such cyber transactions. Some criminals are already using online gambling as a cover for money laundering over the internet, the FATF said in its annual report on money laundering methods. Internet gambling not only makes it difficult to track money movements, but also to decide which jurisdiction has authority over a case.

The largely unsupervised electronic funds transfers inherent in online gambling can be exploited by criminal interests to launder criminal proceeds at the obscure "layering" stage of money laundering. Characteristics of internet gambling such as the volume, speed, and international reach of internet transactions and the offshore locations of internet gambling sites, promote a high level of anonymity and give rise to complex jurisdictional issues. Banking and gaming regulatory officials do not view internet gambling as being particularly susceptible to money laundering, especially when credit cards, which create a transaction record and are subject to relatively low transaction limits, are used for payment. Likewise, credit card and gaming industry officials did not believe internet gambling posed any particular risks in terms of money laundering.²¹ The risk, of course, intensifies when fund-transfer services, wire transfer and digital currencies are used, or where financial institutions accept an internet gaming entity as a direct customer.

Beyond organised crime, some legitimate companies have ended up in serious trouble by failing to comply with foreign states' laws where gambling is prohibited unless licensed locally in particular in the US who charged Pokerstars, Full Tilt Poker and Cereus (Absolute Poker/Ultimate Bet) with legal violations.

Before the US Government crackdown on online poker websites, there were around 2 million people playing poker for money on the internet in the US. After the action, the number of players dropped to around 500,000 with more expected to follow once accounts had expired. US poker players represented 49% of the 2006 global market and by 2011 after government intervention around 7%.

Charities & Not For Profit Organisations

"You shall give the due alms to the relatives, the needy, the poor, and the travelling alien..."

The Holy Koran

Introduction

Charitable giving and "good works" are a key tenet not only of the Islamic tradition but of many faiths including Hinduism, Judaism and Christianity and a major part of the way many secular people contribute and add value to the global community. Raising money for good works, particularly humanitarian relief in the major trouble spots of the world provides literally a lifeline for many. Whilst the vast majority of charitable donations are made and used for legitimate projects and make a tremendous difference to the lives of millions of people around the world, some funds inevitably may benefit illegitimate groups, by either directly or indirectly supporting terrorist groups or insurgent activity.

Definition / Description

Charities and Not For Profit Organisations ("NPOs") are organisations which do not operate for commercial profit or gain or for the direct or indirect profit or gain of its individual members or donors. The funds of such an organisation must be used to carry out the purposes of the charity or NPO, such purposes being either cultural, educational, religious or even professional. Tax exemptions are (where appropriate) often granted for registered charities or NPOs and contributions to them by donors are often tax deductible. Charities and NPOs accept funds for their activities and services from sources which include: public sources including government and supranational organisations and their agencies, the general public, legal entities, or single donors.

Examples of well known charities or NPOs include governmental, supranational and national bodies such as, the UNHCR, UNICEF and USAID, international organisations such as the International Red Cross and Red Crescent Organisations, Medicine Sans Frontier, Save the Children, the Salvation Army and Islamic Aid.

A subset of an NPO is Non-Governmental Organisation or NGO. NGOs perform on a voluntary basis, independent of government and have, in contrast to charities and NPOs, primarily political or quasi political or professional agendas which focus for example on particular causes bringing citizens to government, serving as early warning mechanisms and helping

monitor and implement international agreements. Some of the best known are Amnesty International, Human Rights Watch and Transparency International (TI), World Wide Fund for Nature (WWF) as well as the US based National Rifle Association (NRA) the American Israel Public Affairs Committee (AIPAC) being examples of the issue type of NGOs and the International Air Transport Association (IATA), the International Chamber of Commerce (ICC) and the International Organisation for Standardisation (ISO) being examples of professional representation NGOs. In the private foundation space the world's largest are the Gates Foundation (US\$37.4bio); INGKA Foundation (US\$36bio); and the Wellcome Trust (US\$22.1bio).

The definition/description of charities and NPOs including NGOs excludes a trust, foundation, domiciliary company or other legal entity established for or on behalf of an individual or family group. For more details see Part 2, Section 2, Sub-section 2, Gatekeepers below.

Money Laundering/Terrorist Financing Risks

The use of charities and or the misuse of charitable donations has been cited by FATF as a main source of terrorist financing. The UN as well as governments including the US and EU and elsewhere have also identified particular charities that they claim financially supported terrorist groups.

Whilst the concerns raised by FATF and government designations of certain charities appeared following the 9/11 attacks on America by Al-Qaeda and other major international terrorist atrocities like the 2003 Israeli bus bombings by Palestinian Terrorist Groups such as Hamas and Tamzin Fatah, the London 7/7, Madrid 3/11, and 2002 Bali bombings, the focus has been on the so called Islamic terrorist groups.

Whilst this focus is natural, the existence and operation of the Irish Northern Aid Committee (NORAID), a charitable front founded in the US to support IRA volunteers in their war against British Rule in Northern Ireland, for more than two decades from the 1970s and more recently the designating of the Tamil Rehabilitation Organisation (TRO) by the US and European governments in 2007 show that the misuse of charities for terrorism financing is not limited to the Islamic world. The US Department of Treasury stated that "TRO passed off its operations as charitable, when in fact it was raising money for LTTE ("Tamil Tigers") responsible for heinous acts of terrorism. In the US, TRO has raised funds on behalf of the LTTE through a network of individual representatives and TRO was the preferred conduit of funds from the US to the LTTE in

Sri Lanka".

It is not surprising though that Islamic charities, over the past decade have faced the most scrutiny. Charity forms a very important part of Muslim law and tradition. There is a recognised religious duty in the Muslim world to provide a set portion of earnings or assets for religious or charitable purposes (Zakat), and otherwise to support charitable works through voluntary deeds or contributions (Sadaqah). In countries like Saudi Arabia or the United Arab Emirates that have no established income tax system, the Zakat substitutes as the principal source of funding for religious, social and humanitarian organisations and activities.

The funds are collected by the government, or through local mosques and religious centres. Sadaqah contributions are also made directly to established Islamic charities. As both Zakat and Sadaqah are viewed as personal religious responsibilities there has traditionally been little or no government oversight of these activities. Donations in large measure remain anonymous. Elsewhere through the Islamic diaspora, particularly in the US and in Europe, these established principles of giving have generated significant sums of money for large organisations, often anonymously.

There are two major ways that charitable donations can be abused. Firstly, a Charity can be set up purely as a "cover" for terrorist fund raising and support. Secondly, it can be set up for legitimate reasons but has been wholly or partially established to move or distribute money for illicit purposes. Al-Qaeda, Al-Qaeda affiliates and other terrorist groups such as Hamas and Hezbollah have taken full advantage of the lack of oversight to open their own front charities and to solicit funds through collection boxes at mosques, Islamic centres and elsewhere. These groups have also placed operatives in key positions within established Charities to further their causes. Funds raised or allocated by or for Al-Qaeda, for example, are co-mingled, maintained and transferred with funds designated for legitimate relief and developmental activities. Their ultimate use in supporting the agenda of the terrorists group comes later when the moneys are transferred or diverted to terror connected recipients.

In 1996 the CIA issued a Report on NGOs with terror links, identifying a number of charities with links to Bosnian fighters during the wars in former Yugoslavia, some of which claimed connections with terrorist groups designated as such by the US. Examples of NGOs so identified included the Philippine and Indonesian branches some offices of the International Islamic Relief Organisation, the Bosnian and Somalian offices of the Al Haramain Islamic Foundation, Muwa-

faq Foundation.²¹ For more details see Part 2, Section 7 below.

Whilst charities and NPOs are now subject to government oversight, until fairly recently this oversight was rudimentary. Still in many parts of the world, this oversight remains likely light touch.

During the so called "war on terror" a number of charities have been accused by some of ties to terrorism. The following have been accused in some form:

Charities accused of ties to terrorism in US led "War on terror"		
Name	HQ	By
Afghan Support Committee	Pak	US
Al-Haramain Foundation	Saudi	US
Al Kifah Refugee Centre	US	Spain
Al Wafa al Igatha al Islamia	Afgh	US
Benevolence Int Foundation	US	US
Bosanska Idealna Futura	Bos	US
Global Relief Foundation	US	US
Health & Education Project Int	Can	Canada
Holy Land Foundation	US	US
Human Appeal International	UK	US
Human Concern International	Can	US
Int Islamic Relief Organisation	Saudi	US
Interpal	UK	US
Int Humanitaere Hilfsorg	Ger	Ger
Jamaat al Dawa al Quran	Afgh	US
Jamat al Tabligh	Afgh	US
Maktab al-Khidamat	Afgh	US
Muslim Aid	UK	US
Soc Revival of Islamic Heritage	Kuw	US
Sanabala Charitable Com	UK	US
Tamils Rehabilitation Org	Can	US
Lakemba Mosque	Aus	Aus

Source: Wikipedia
http://en.wikipedia.org/wiki/List_of_charities_accused_of_ties_to_terrorism

Gatekeepers

"Gatekeepers [including lawyers, fiduciaries and company service providers] are useful for money launderers due to their access to the financial systems, and area of expertise. Gatekeepers may be involved in money laundering for themselves or third parties."

Wolfsberg Group "Guidance on a Risk Based Approach for Managing Money Laundering Risks"

Introduction

Criminals require the services of these professionals to set up corporations, structures and vehicles to move and launder criminal monies out of sight, across jurisdictions, to advise on how to avoid and or circumvent the law and how to absorb the proceeds of crime within businesses and prepare illegitimate accounts. They may also add a veneer of respectability and provide credibility to a criminal enterprise. Notwithstanding this, the overwhelming majority of professionals, knowledgeable as they are and risk averse by nature, avoid such dealings and involvement.

Definition/Description

FATF have identified a class of businesses they call, "Designated Non-Financial Professions and Businesses (DNFPBs)" being professions and businesses that are seen as being attractive to money launderers and these are: casino's (when their customers engage in financial transactions above US\$/€3,000), lawyers, notaries, other independent legal professionals and accountants and trust and company service providers, dealers in precious metals and stones (when their customers engage in cash transactions above US\$/€15,000) and real estate agents.

Lawyers, notaries, other independent legal professionals and accountants are to be caught when they prepare for or carry out transactions for their client concerning the following activities: (i) buying and selling of real estate; (ii) managing of client money, securities or other assets; (iii) management of bank, savings or securities accounts; (iv) organisation of contributions for the creation, operation or management of companies; (v) creation, operation or management of legal persons or arrangements, and (vi) buying and selling of business entities.

Trust and company service providers are caught when they prepare for or carry out transactions for a client concerning the following activities: (i) acting as a formation agent of legal persons; (ii) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; (iv) acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; (v) acting as (or arranging for another person to act as a nominee shareholder for another person.

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are generally not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. Also where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

The Wolfsberg Group "Guidance on a Risk Based Approach for Managing Money Laundering Risks" identified some characteristics of customers with potential higher money laundering risks, including, "Accounts for 'gatekeepers' such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution."

Money Laundering/Terrorist Financing Risks

Gatekeeper's remain a common element in complex and/or opaque structures. As long ago as 1996, the FATF VII – Report on ML Typologies referred to so called "middle persons", such as lawyers, who assist in schemes such as depositing large amounts of cash, in this example that were tied to Russia and Eastern Europe, into the financial institution and then transferring the funds out of the country. Furthermore, the establishment and use of trusts has also been well documented, as noted in the FATF report titled, Money Laundering using Trust and Company Service Providers. The use of Trusts by criminals make it difficult for authorities investigating criminal activities to acquire the necessary insight and connections required for a successful investigation and prosecution especially when the investigation is from overseas. The FATF also noted, in their 2010 Global Money Laundering & Terrorist Financing Threat Assessment report, the increased use of these professionals, referred to as gatekeepers, for money laundering cases, "especially those involving significant financial fraud and organised crime. Criminals may seek out the gatekeepers to minimise suspicion of criminal activities due to the gatekeeper's reputation, presumed

ethical standards, and their expertise in disguising suspicious transactions/activity, as well as “take advantage of the professional secrecy obligations that may apply to the gatekeeper.”

In 2010 the US Senate Permanent Subcommittee on Investigations held hearings on “Keeping Foreign Corruption out of the US” and issued a report with the same title, which detailed four case studies in which US banks and professionals facilitated transactions that laundered money for foreign corrupt officials and their families. One of the cases involved *Teodoro Obiang*, the son of the President of Equatorial Guinea, who used his lawyer’s services to launder over US\$110mio in illicit funds through the lawyers clients account and through accounts of various shell companies. The Subcommittee used its findings from the hearing and the report to support regulations on attorneys, at least those involved in financial transactions, so called, “gatekeepers” to engage in customer due diligence, record keeping and reporting of suspicious activities by their clients. According to the FATF, “If one looks at the types of assistance that these professionals may provide, it is apparent that some of these functions are the gateway through which the launderer must pass to achieve his goals. Thus the legal and accounting professionals serve as a sort of “gatekeeper” since they have the ability to furnish access (knowingly or unwittingly) to the various functions that might help the criminal with funds to move or conceal.

Another meaningful example of how Gatekeepers can be used to facilitate money laundering is the case of *James Ibori*, a former Nigerian governor arrested and convicted of laundering corrupt monies.

Notwithstanding the identified risks and vulnerabilities presented by some so called “gatekeepers”, the organised legal and accounting professions have either attempted to avoid accepting many of the same obligations that are applied to financial institutions or where obligations are imposed sought to limit these and or contributed little in terms of suspicious activity Reporting. Many lawyers and accountants continue to claim that there is little established empirical connections between laundering and lawyer or accountant involvement.

Whilst it appears true that there is little empirical data there are some studies and data which albeit limited and small samples, nevertheless indicate that gatekeepers can and should play a role.

In a study called “My Brother’s Keeper: An Empirical Study of Attorney Facilitation of Money Laundering through Commercial Transactions”, the authors, Lawton

P. Cummings and Paul T. Stepnowsky, found that albeit in a small sample, in the US on the courts second circuit in 2009 of all cases prosecuted which included charges of money laundering, lawyers were involved in facilitating money laundering in 25% of the cases. Of that 25%, 40% related to direct activity by lawyers who were prosecuted themselves for active crimes and 60% where a lawyer was used albeit seemingly where the lawyer was an unwitting actor. Of this 60%, over 80% involved the purchase of real estate with, in many cases, the money passing via a lawyer’s account. In several of the cases, the crime related to mortgage fraud schemes. In some others the property was placed in the name of a third party to obscure the criminal’s identity and ownership of the asset. Only one case actually involved the creation of a legal entity for a criminal party. Finally the predicate crime which led to lawyer involvement in a transaction to launder the money where overwhelmingly white collar crime.

Whilst the data is not conclusive it indicates that in this case lawyers as gatekeepers may be an important asset in the fight against money laundering or alternatively can act as effective facilitators of financial crime. Some hide behind codes of ethics, laws of privilege and confidentiality which leaves law enforcement at a considerable disadvantage.

Whilst in this study offshore companies did not feature highly, they have been a feature in many of the most notorious money laundering schemes, but at the same time as they have been used for illegitimate purposes, like cash, that should not imply that their principal purposes and usefulness should be questioned.

Offshore Companies

Offshore companies are called many things, though the most popular name is IBC – “International Business Company,” though other names are frequently used such as “non-resident companies”, “exempt companies”, “special license companies”, PIC’s or “Private Investment Companies”, “Shell Companies”, “Off the Shelf Companies”, “Brass Plate Companies”, and no doubt numerous more. The companies come in two types, ordinary registered share companies and bearer share companies, the latter being perceived as presenting ever greater money laundering risks. There are alternatives to companies as legal structures, that are owned or controlled ultimately largely by individuals, including: trusts, foundations, anstalts and stiftungs amongst the most well known.

One of the most popular offshore vehicle of all appears to be the IBC, incorporated in the British Virgin Islands (BVI), following the introduction of a zero-tax level for

all business in 2004. There are a number of legitimate primary purposes for these companies. One is tax minimization and the others include asset protection and confidentiality. Whilst these purposes may exist independently they often interlap and complement each other.

Whilst the BVI is widely acknowledged as having the greatest number of offshore companies registered (number three in total and number one by population per head - see below) there are several dozens of countries worldwide offering different sorts of financial and tax benefits.

Top Locations for establishing IBCs			
No	Location	Numbers	per 100 pop
1	Hong Kong	1,045	15
2	Delaware	945,000	104
3	BVI	473,000	1,995
4	Cayman Is	92,000	161
5	Jersey	33,000	34
6	Bermuda	17,000	25

Source: The Economist as at December 2012

The BVI IBC has a number of attributes which has made it particularly attractive, including: (a) total absence or minimum levels of taxation; (b) confidentiality, due to there being no sensitive personal information available on public files; (c) secrecy protection and few effective international information-sharing agreements; (d) corporate flexibility: no paid-up capital requirements, no requirement to state operational objects, minimum conditions on directors and shareholders, fast incorporation; (e) ease of management – shareholders’ meetings can be held anywhere, including by electronic means, flexible decision making process (f) minimum reporting – no audits, no tax reports, no financial information on the public files.

Gatekeepers, such as lawyers, notaries, accountants or company formation agents will normally be used to establish such vehicles and in so doing should check the bona fides of their customers.

Many offshore companies kept pre-prepared IBCs “on the shelf” awaiting activation. Often IBCs have other IBCs as corporate directors, officers and shareholders, with some describing these shells, within shells, within shells, like Russian Matryoshka dolls, which can make it difficult to identify true beneficial owners.

Once an IBC or other offshore company or other vehicle or legal entity is established, and despite the limited amount of public disclosure the company or entity

will usually open a bank account, though unless there is some connection with the jurisdiction of the country where the IBC is incorporated the account will usually be opened offshore, for example in a financial centre or in a country that is known as a “financial centre”. Examples of widely known financial centres are UK (City of London), Manhattan, in New York City; Switzerland, Austria, Luxembourg, Singapore, Cayman Islands, the Bahamas and the Channel Islands.

Notwithstanding the limitations on disclosure on acquiring an IBC, to open a bank account in the name of the offshore company, is only possible at a reputable bank if detailed personal and business information also about the owners and controllers of the offshore company are provided. In particular, the bank will need to know and identify the actual beneficial owner(s) of the offshore company. All such persons, as well as everyone who will be granted account signatory rights, will have to be properly identified and will have to provide a number of documents - such as a certified passport copy, perhaps a reference, and explain the purpose of the company and the expected usage of the account and the source of funds for moneys being credited to the account.

Foundations including Anstalts and Stiftungs

Foundations are the creation of civil law countries which include virtually all Continental countries apart from Cyprus, Gibraltar and Malta and have also emerged in places like Panama.

The first key benefit of a foundation is that it owns its own assets and not, as with a private limited company, owned by its investors/shareholders - be they beneficial owners or nominees. The second key benefit of a foundation is that it will be treated as analogous to a private limited company at least under English Law and most likely by other major common law countries. The closest analogy to a foundation is the common law discretionary trust but unlike a trust, a foundation is generally treated like a private limited company, without applying to it the provisions of trust legislation applicable in most common law countries. It is also often possible for a founder (or ‘originating party’ if the funds are not directly lodged) to maintain greater control over lodged foundation assets than in the case of a common law trust. Most foundations will have not only a charter document (generally recorded with a companies registry) but also a regulatory governing document. This, whilst not on public record, is vital if an individual’s bespoke provisions are to be achieved especially in respect of beneficiary and determination issues.

Whilst public foundations can be established in virtually any civil law country, the three most popular jurisdictions for private interest foundations for both legal and tax reasons are Liechtenstein, Panama and Switzerland.

High Value Goods Dealers

"The use of large cash payments has repeatedly proven to be very vulnerable to money laundering and terrorist financing."

EU Third Money Laundering Directive 2005 preamble

Introduction

Businesses that offer high value luxury goods should recognise that not only are their products acquired by those with legitimate wealth, but they are also a target of criminals, both from a pure desire for commercial consumption, to improve perceptions about social standing but also by criminals wishing to launder the proceeds of crime or convert proceeds from cash into non-bankable assets. Businesses that offer high value luxury goods such as works of art, auctioned items, cars, planes, jewellery, real estate, and yachts and other property such as watches, wine and champagne, thoroughbred horses, pedigree dogs, to name some of the most important, need to take care that the purchaser and/or if the price is being paid in cash is legitimate.

Any product that offers the opportunity to criminals to convert cash or other valuables can assist criminals to launder their ill gotten gains; High Value Goods, offer both a more attractive alternative asset class than traditional financial products, and retain elements of confidentiality and convertibility as well as being used to launder very large sums.

Definition/Description

FATF have identified a class of businesses they call, "Designated Non-Financial Professions and Businesses (DNFPB's)" being professions which are seen as attractive to money launderers and these are: Casino's, (when their customers engage in financial transactions above US\$/€3,000), lawyers, accountants and trust and company service providers, dealers in precious metals and stones (when their customers engage in cash transactions above US\$/€15,000) and real estate agents.

The EU in its Third Money Laundering Directive 2005 have gone further than the FATF requirements and included a broad category of dealers who trade in goods (but not services), where payments in cash are made in excess of €15,000, and who need to register and implement an AML programme and file SARs as appropriate. The EU in its proposed 4th Money

Laundering Directive is intending to reduce this to €7,500. Other major jurisdictions outside the EU have yet to follow this broad more extensive approach, instead largely focussing on regulating DNFPBs alone.

Money Laundering/Terrorist Financing Risks

As well as art, criminals have invested or converted their ill-gotten gains or illicit funds into all kind of goods, but the most important appear to be planes, boats, particularly yachts, luxury automobiles or premium sport cars, real estate, wines and champagne, animals, watches, jewellery and of course apparel including clothes and shoes through auction or by private sale. The special attraction of these goods is not only that they are expensive and therefore guarantee a significant level of turnover of illicit funds, but they are also prime status symbols, which to some for example, kleptocrats, are important to show to the world the wealth accumulated in the most direct manner possible.

Top 10 most powerful luxury brands in the world		
Brand	Overall Brand Value	
1 Louis Vuitton	US\$19.78bio	
2 Hermes	US\$8.47bio	
3 Gucci	US\$7.59bio	
4 Chanel	US\$5.55bio	
5 Hennessy	US\$5.37bio	
6 Rolex	US\$4.74bio	
7 Moet & Chandon	US\$4.28bio	
8 Cartier	US\$3.96bio	
9 Fendi	US\$3.20bio	
10 Tiffany & Co	US\$2.38bio	

Source: Millward Brown Optimor (part of WPP) - 2009

The Annual Bain Luxury Goods Worldwide Market Study published in October 2012 includes figures on global spending for a number of high value goods. On luxury cars, the spending is US\$381 bio (up 4% compared to 2011), and for yachts US\$9 bio (up 2% compared to 2011). Those are impressive figures and give an indication on the size of the global industry supporting the market of luxury goods.

Whilst much of the sales of these luxury items are legitimate, clearly the market is deep enough for criminals to exploit. Beyond kleptocrats, organised criminal gangs like the drug trafficking cartels in Mexico and Colombia have invested vast amount of their illicit funds into luxury items. For example, the deceased

Colombian drug lord, Pablo Escobar, was well known for his extensive and highly prized car park and Mexican Cartels have taken things a step further, in addition to seeking luxury goods, they have acquired boats and planes of the more practical size, using these to transport drugs from the producing countries to intermediate locations and then on to the US.

Auctions

Whilst auction houses are famous for their sales of art, much more than art is sold by auction, including jewels and real estate, livestock, wine and watches. Traditional auction houses, such as Christie's and Sotheby's with a long heritage going back over hundreds of years, hosting auctions of the world's finest art and artefacts, dominate these public sales in which goods or property are sold to the highest bidder. At the end of 2011, Sotheby's had an auction of contemporary art with sales of US\$200mio in a single night. Yet, the best year for a traditional auction house went to its rival Christie's, which generated approx US\$6bio. Nevertheless, with new technology, the auction business albeit not really focussed on the luxury market which dominates is eBay, which started out with an idea for a simple auction system, and now generates US\$150bio in sales a year. The "micro" auctions that typify eBay's auction model are an alternative albeit more volume related vehicle to launder illicit funds as are the online games that involve virtual auction houses that facilitate the transfer of real money. The following provides a brief summary of certain luxury markets and some of the most expensive purchases to date.

Art

Works of art may include a multitude of disciplines ranging from fine art in the form of painting, photography and sculptures to literature and music. For AML purposes, the term art has to be thought of in broad terms to include culturally significant antiquities. In addition to money laundering involving such items, one should bear in mind other crimes related to art and antiquities. For example, see Part 1, Section 1, Fraud and Environmental Crime.

The most expensive paintings purchased include "the Scream" by Edvard Munch, which sold at Sotheby's at auction in 2012 for a record US\$120mio (but which has recently been topped by the sale of Francis Bacon's Lucian Freud which sold for US\$142mio). The painting is actually one of four versions painted by Munch and the only version whose frame was hand-painted by the artist to include his poem, detailing the work's inspiration. The Scream or the Screams have been the target of a number of thefts and theft attempts, with two of the four being stolen but retrieved later. The previous

record for the most expensive work of art sold at auction had been held by Picasso's Nude, Green Leaves and Bust, which went for US\$106.5mio at Christie's two years prior in 2010 and before that the previous record was held also by Picasso's Boy with a Pipe, a painting that sold for US\$104mio. When accounting for inflation, the highest price paid for art at an auction is still held by Van Gogh's Portrait of Dr. Gachet, which sold for US\$82.5mio in 1990, or about US\$147mio in 2012 equivalent money. Outside of auction, Jackson Pollock's Number 5, painted in 1948 reached a price of US\$140mio and whilst unconfirmed there have been reports that "The Card Players" by Cézanne, sold privately for US\$250mio in 2011. Beyond paintings, drawings and even photographs have commanded high prices. The most expensive drawing was sold at auction in 2009 by Christie's in London. Raphael's Head of a Muse, a black chalk drawing on paper, sold for almost US\$50mio. Andreas Gursky is well-known for his stunning full-color landscapes, though the world's most expensive photograph, costing US\$4.3mio was Rhein II a large print of the famous German river, which seems to only include green and grey. As far as sculpture goes, the record here goes to Giacometti's sculpture of the "Walking Man I" for US\$104.3mio, easily beating the most expensive sculpture from antiquity, the Roman-era statue, "Artemis and the Stag" which sold in 2007 for US\$28.6mio. As far as books or manuscripts are concerned, the highest price recorded for a printed book was until recently a copy of John James Audubon's "Birds of America" which sold for US\$1.5mio at Sotheby's in 2010. This was topped in 2013 by a book which sold for just under US\$14.2mio also at Sotheby's in New York. The book a translation of the Biblical psalms, from the original Hebrew, called, "The Bay Psalm Book", was printed by Puritan settlers in Cambridge, Massachusetts in 1640 just 20 years after the Pilgrims landed at Plymouth and is considered to be the first book printed in what is today the United States of America. Notwithstanding this sale of a printed book, the auction record for any book goes to the Leonardo da Vinci Codex Hammer, a personal notebook of scientific writings and diagrams, which sold for US\$30.8mio at Christie's auction house in 1994.

Jewels and Real Estate

For more details see Precious Metals and Stones Dealers and Real Estate Agents below in this Part 1, Section 2, Sub-section 2.

Planes, Automobiles and Yachts

Luxury private jets range from about US\$31mio for a Bombardier Global 5000 to US\$65mio for the Gulfstream G650. For the seriously wealthy there is a trend to take even Boeing and Airbus large passenger

jets and upgrade them, fitting them out for personal use. Airbus lists a price of US\$68mio for its smallest single-aisle A318 to about US\$245mio for the twin-aisle A350, which is under development.

For Boeing the most expensive private jet is the Boeing 747-8 VIP at a price of US\$295mio. Boeing has sold seven 747-8 VIPs where the interiors are fitted out by the customers own designers, to look more like a luxurious home than like a plane, which can add still millions more onto the total cost.

At Airbus, the company lists its new A380 double-decker at US\$389.9mio before any upgrades. After taking the order in 2007, Airbus delivered the behemoth jetliner to a single customer in 2013, the Saudi Prince Alwaleed bin Talal, the Chairman of The Kingdom Holding Company. It is considered the most expensive personal jet, with a final price in excess of US\$500mio. The original plans included a garage for two Rolls-Royces, a stable for horses and camels, a pen for hawks and a prayer room that rotates so it always points toward Mecca.

Other notable large jet owners include Google's founders, Sergey Brin and Larry Page, who bought a secondhand Boeing 767 in 2005 and turned it into their private plane and Hollywood actor, John Travolta who somewhat differently flies his own vintage Boeing 707.

The most expensive new car in the world is the Bugatti Veyron Supersport. This Bugatti is made in France and has a 16 cylinder – 1,200 horsepower engine. The Bugatti hits 0-60 mph in 2.6 seconds with a top speed of 268 mph and a price of US\$2,600,000. Vintage classic cars can cost much more however. For example, the Mercedes-Benz W196, which won the Grand Prix in 1954 and 1955, sold at auction in 1990 for US\$24mio recently topped by the sale for US\$26mio for a Mercedes Benz W196R (driven by Fangio in F1 wins in 1954 in Germany and Switzerland) and a 1962 Ferrari 250 GTO which became the most expensive car ever when it was sold in the UK to a private collector for US\$35mio.

Motorcycles naturally are less expensive, though the most expensive Motorcycle, the "Dodge Tomahawk V10" costs US\$700,000. It is a 1,500lb. motorcycle with four wheels, has a Dodge Viper's V10 engine and can go from zero to 60 mph in 2.5 seconds, with a top speed estimated to be more than 300mph.

The world's most expensive private yacht is the Eclipse, which cost Russian Oligarch, Roman Abramovich, US\$590mio. Built in 2010 and is just over 538ft long,

the Eclipse can accommodate up to 30 guests in 15 cabins and also cater for 75 crew members. It has two helipads, 11 guest cabins, two swimming pools, three launch boats, an aquarium, and a minisubmarine that can dive to 50 meters below the ocean surface. The master bedroom and bridge have bulletproof glass, and the security system includes missile detection systems that warn of incoming rockets. Interestingly it can be privately charted for approx US\$2mio per week, plus expenses (notably US\$650,000 for a single fuel fill-up).

The yacht that comes in second place was built for Prince Jefri Bolkiah of Brunei and is called, "Dubai" measuring 162 metres long. The seven decks of the yacht house, among other things, has a mosaic swimming pool and multiple Jacuzzis. Not only that, the ship can accommodate a 9.5 ton helicopter and two smaller 10-meter long tenders. A glass staircase adds brilliance to this most lavish and expensive yacht.

A long way behind both Eclipse and Dubai are two Yachts the first a new Yacht shown at the 2012 Singapore Boat Show and the second owned by an American businesswoman at the Dubai Boat Show. The first the "Helix" is priced at US\$44.5mio and is 45 meters long, whilst the Andiamo is shorter at 42.5 meters long and costs US\$24.5mio. The Andiamo is called the Rolls-Royce of the sea.

Animals

Horse racing, and equestrian sports and skill have a long and distinguished history, with thoroughbred racing long popular amongst the rich and noble earning it the title "Sport of Kings." The most expensive horse purchased at auction was called, "Green Monkey" and was the descendant of two US Kentucky Derby winners, costing US\$16mio. Unfortunately the horse ran in three races, but only managed one third place. One of the most successful horses of recent times, "Frankel" retired in 2012 unbeaten in his fourteen race career in the UK being billed as the highest-rated racehorse in the world. Whilst he is not for sale, estimates of his value top £100mio. The valuation is based on the his future stud fees, which have been set at £125,000. In his first season as a stallion he will cover approximately 130 mares.

The most popular dog breeds are not the world's most expensive dog breeds, but the luxury dogs rate high at the top of the list. Popular dog breeds change from year to year and from country to country; and so do the most expensive dogs in the world. There are a variety of factors which make dogs expensive. Purity of breed or their rarity can make dogs extremely expensive, alternatively being spotted in the hands of a major celebrity! The most expensive dog ever sold was a red

"Tibetan mastiff" called Big Splash, or "Hong Dong" in Chinese. This most expensive dog ever already stood nearly three-feet-high at the shoulder and weighs more than 180lbs at 11 months old. He was purchased by a Chinese multi-millionaire coal baron for approximately US\$1.5mio and beats the earlier record set by another Tibetan Mastiff called "Yangtze River Number Two" which was sold to a Chinese woman in 2009 for about US\$609,000. Whilst the most expensive cat breed is the Bengal cat, which is a hybrid cat that is a cross between a domestic feline and an Asian Leopard Cat, one of these cats sold for US\$42,000. Still whilst this breed is much sought after, it was a four-year-old former stray cat from Rome, "Tommaso" that could be really considered to be worth a fortune after inheriting approximately US\$13mio from a wealthy owner. Whilst Tommaso can count himself very lucky he cannot be considered unique as he is only the third most wealthy animal on the planet. He is preceded by Kalu the chimp, who was left US\$80mio when his owner passed away and Gunther IV a dog who inherited US\$372mio from a German countess.

Watches

The President of the US, Barack Obama, wears a Tag Heuer 1500 Professional Series. Former President Bill Clinton, on the other hand, sports a Panerai.

No	Most Expensive Watches sold at Auction	
1	Chopard 201-Carat Watch	US\$25mio
2	Patek Philippe Henry Graves Super Complication Pocket Watch	US\$11mio
3	Patek Philippe Reference 1527 Wristwatch	US\$5mio
4	Breguet & Fils, Paris No 2667 Precision Watch	US\$4,682,165
5	Louis Moinet Meteoris Watch	US\$4,599,487
6	Patek Philippe 1939 Platinum World Time Watch	US\$4,026,524
7	Patek Philippe 1928 Single-Button Chronograph Watch	US\$3,637,408
8	Piaget Emperador Temple Watch	US\$3.3mio
9	Patek Philippe 1953 Model 2523 Heures Universelles Watch	US\$2,899,373
10	Cartier Secret Watch with Phoenix Decor	US\$2,755,000

Source: Author

The former French counterpart, once called President bling bling, Nicolas Sarkozy, has a Rolex. In Hollywood, Daniel Craig wears a Rolex Daytona, and not the Omega that is a fixture in James Bond movies. Sylvester Stallone, meanwhile, prefers a Panerai Submersible, while multiple Academy Award winner Tom Hanks has been seen with either an Omega PO or a Rolex Milgauss GV. In the world of sports, Miami Heat superstar and the reigning Most Valuable Player in the National Basketball Association Lebron James has worn an Audemars Piguet Royal Oak Offshore. Whilst there are many reasons to prefer a particular type of watch, accuracy, complexity, adorned jewellery, scarcity or just style, the most expensive watch has many of these qualities though it is more jewellery than watch, being heavily adorned with jewels. It is the Chopard 201-Carat Watch which sold at auction at US\$25mio.

Wine and Champagne

Everyone knows the older the wine, generally, the better it gets up to a point at least. Vintage wines are chosen from some of the most exceptional vineyards and may sell for thousands of dollars per bottle. Some of the rarest bottles in the world have attracted record prices. Considered the most expensive standard bottle is a Chateau Cheval Blanc 1947 that has been given A class status in the Classification of Saint-Emilion wine. According to Christie's wine expert, Michael Ganne, this is the only known bottle in the imperial format and can be kept for another 50 years without any problem. One of the greatest Bordeaux of all time, the bottle was owned by an anonymous Swiss collector. The wine was sold at an auction at Christie's in Geneva and was sold for US\$304,000. Another very expensive wine is the Chateau Lafite-Rothschild 1869. Three bottles of 1869 Chateau Lafite Rothschild were sold in Hong Kong at auction going for US\$232,692 each. The fact that made the bottles rare was they came directly from the Chateau Lafite's cellars.

The single most expensive bottle of wine ever sold was a "Screaming Eagle Cabernet Sauvignon 1992" which was purchased with the proceeds going to charity at the Napa Valley Wine Auction in 2000 by Chase Bailey, a former Cisco Systems executive for US\$500,000. The bottle was a gigantic 6 litre bottle however, so taking size into account the Cheval Blanc is for its size still the most expensive. The most expensive Champagne was the "Heidsieck Monopole Champagne 1907" which were recovered in 1997 from a ship that sank in the Baltic Sea. Over 200 bottles were being shipped to the Russian Imperial family in 1916 but were lost at sea en route. The Ritz-Carlton Hotel in Moscow claimed 10 of the bottles and made them available for sale in 2008, the first being sold for US\$35,000.

Intermediaries

"All things can corrupt when minds are prone to evil"
Ovid, Roman poet active in BC & AD²²

Introduction

Intermediaries have been used throughout history, as buyers and sellers of goods and services have used middlemen to access local markets, including obtaining local market intelligence to gain an advantage over competitors. Increased focus on combating bribery and corruption has resulted in scrutiny over the use of middlemen in all sorts of business sectors. Intermediaries are perhaps the most prominent in sectors trying to access the emerging markets and procurement of government contracts, especially where such contracts relate to the natural resources or the energy sector. This is not to say, however, that every time an intermediary is appointed, that the arrangement is suspect or is performed with criminal intent.

Definition/Description

According to the Wolfsberg Group in their "Guidance on a Risk Based Approach for Managing Money Laundering Risks", the "use or involvement of intermediaries within the relationship" was identified as posing increased risks. The Wolfsberg Group Anti Corruption Guidance²³ defines an intermediary as "third parties that are engaged, directly or indirectly, by the financial institution to act on their behalf to find, introduce, obtain or maintain business, clients or licences for the financial institution, or who introduce the financial institution to government officials or government enterprises, irrespective of whether a transaction is completed". The OECD Working Group on Bribery in International Business Transactions provides a broader definition²⁴ of what an intermediary is, that is "a person who is put in contact with or in between two or more trading parties" and states that "the intermediary can act as a conduit for legitimate economic activities, illegitimate bribery payments, or a combination of both". Intermediaries can be: (i) agents; (ii) sales representatives; (iii) consultants or consulting firms; (iv) suppliers; (v) distributors; (vi) resellers; (vii) sub-contractors; (viii) franchisees; (ix) joint venture partners; (x) subsidiaries, and (xi) other business partners including lawyers and accountants.

Money Laundering/Terrorist Financing Risks

Whilst the use of intermediaries is commonplace in commerce, and the vast majority perform legitimate services, often helping with technical expertise, or local knowledge, communication, custom, practice or contacts especially in far away places, Intermediaries can

also be used as part of a corrupt transaction.

The OECD²⁵ states that intermediaries can legitimately be used in order to assist/give guidance to companies looking to work in unfamiliar environments, particularly new geographical jurisdictions. In these cases, intermediaries perform a legal and vital service, giving guidance on cultural, legal and financial complexities and obligations, or providing access to closed/insular markets. They can also act as local employees when it is impossible or difficult for an international company to relocate or employ other individuals, due to legal or financial restrictions. The issue therefore, is intent, and whether there is an intent to use an intermediary to corruptly influence key decision makers, be they government officials or other corporations.

For example, an important public official in a position of power to influence business decisions may direct a tendering company to deal first with a nominated intermediary, perhaps someone related to the family of the official, a friend or other third persons act as an intermediary, someone who will be paid a large commission, perhaps upfront, for very limited actual services, with the expectation that the commission payment will find its way to or benefit the official.

Whilst there is likely to be no written agreement or direct evidence of a bribe, the set up and circumstances are highly suspicious. The company paying the intermediary will generally know, or at least should reasonably suspect, that the payment being made is a bribe. The corrupt official will elect to have payments sent on from the intermediary to a family member or a close associate typically in an offshore jurisdiction.

An integral part of any successful money laundering corruption scheme is to create distance: for corruption between the corrupt individual and their deeds, and in money laundering between the origin of the criminal assets and their "clean" end, in order to evade detection, prosecution and conviction. Crucial to both these ends is the use of intermediaries that can create distance between and obscure the origin of corrupt/criminal payments or instructions.

Corrupt PEPs will, for example, take great pains to disguise the identity and the source of the funds in order to place corrupt money in the financial system without suspicion or to receive illicit funds/bribes. There have been numerous examples in corruption cases, where the corrupt individual has used an intermediary in order to access financial services, or to act on their behalf.

Money Services Businesses

"International money remittances were estimated at US\$400bio in 2012 much of which flowed via Money Services Businesses largely from immigrant workers sending money home to family and friends."

World Bank's November 2012 Migration and Development Brief

Introduction

A 2005 US DEA study determined that alongside; (i) bulk currency smuggling and the use of US based money remitters, the other major money laundering threat relating to the movement of drug proceeds to Mexico were the Mexican currency exchange houses, referred to as Casa de Cambios and Centros Cambiario. In 2006 FINCEN advised all US financial institutions formally about this threat. In 2010, US and Saudi Arabia, respectively, were the top two senders of remittances, with more remittance providers in the US than the next nine Countries combined.

Number of MSBs providing Remittances		
1	US	25,000
2	UK	2,818
3	HK	2,008
4	Mexico	1,085
5	Dermark	334
6	Argentina	122
7	Sweden	96
8	Finland	70
9	Spain	46
10	Germany	38

Source: FATF 2008

to individuals who may not have ready access to the formal banking sector. MSBs are often closely located to particular neighbourhoods which they serve, particularly immigrant populations where cheque cashing, currency exchange and international remittance services are required, or close to borders where tourists and commerce flow, they often offer cheaper rates for their services than banks, and they do not require the opening of an account to process transactions. As far as pure currency exchangers Poland, the US and Mexico make up the top three.

Currency Exchange Numbers		
1	Poland	4,193
2	US	3,294
3	Mexico	2,757
4	Spain	2,256
5	HK	2,008
6	UK	1,404
7	Serbia	1,781
8	Croatia	1,242
9	Ukraine	1,104
10	Georgia	1,050

Source: FATF 2008

According to the World Bank's November 2012 Migration and Development Brief international money remittances were estimated at US\$400bio in 2012 much of which flowed via MSBs largely from immigrant workers sending money home to family and friends. Estimates that remittances to developing nations will continue to grow by 6.5% in 2013.

Remittances: Top 10 recipient countries		US\$bio
1	India	55
2	China	51
3	Israel	20
4	Mexico	21
5	Philippines	17
6	Poland	14
7	Bangladesh	11
8	Nigeria	10
9	Pakistan	9
10	Morocco/Vietnam	7.5

Source: UN / World Bank 2008 / 2009

In Asia the big net recipients of remittances are India, China, Philippines, Bangladesh and Vietnam. Most of the remittances happen by the conventional channel of agents, like Western Union, UAE Exchange, MoneyGram or Xpress Money Services. However, with the increasing relevance and reach of the Internet, online and mobile phone money transfers from companies such as Remit2India and Xoom.com have grown significantly.

In Latin America and the Caribbean, remittances play an important role in the economy of the region, totalling over US\$ 66.5bio in 2007, with about 75% originating in the US (95% when it comes to Mexico). This total represents more than the sum of foreign direct investment and official development aid combined. In seven Latin American and Caribbean countries, remittances even account for more than 10% of GDP and exceed the dollar flows of the largest export product in almost every country in the region. Percentages ranged from 2% in Mexico, to 18% in El Salvador, 21% in Honduras, and up to 30% in Haiti.

A significant study conducted by the Inter-American Development Bank (IDB) in 2004 provides useful insight into remittance and related migration patterns between Latin America and the US. The study reveals that over 60% of the 16.5 million Latin American-born adults who resided in the US at the time of the survey regularly sent money home. The remittances sent by these 10 million immigrants were transmitted via more than 100 million individual transactions per year and amounted to an estimated US\$30bio during 2004. Each transaction averaged about US\$150–US\$250, and, because these migrants tended to send smaller amounts more frequently than others, their remittances had a higher percentage of costs due to transfer fees. Migrants sent approximately 10% of their household incomes; these remittances made up a corresponding 50-80% of the household incomes for the recipients. Significant amounts of remittances were sent from 37 US states, but 6 states were identified as the “traditional sending” states: New York (which led the group with 81% of its immigrants making regular remittances), California, Texas, Florida, Illinois, and New Jersey. The high growth rate of remittances to Mexico (not the total amount) is unlikely to continue. In fact, according the Mexican central bank, remittances grew just 0.6 during the first six months of 2007, as compared to 23% during the same period in 2006. Experts attribute the slowdown to a contraction in the US construction industry, tighter border controls, and a crackdown in the US on illegal immigration.

Remittances to Africa play an important role also to national economies, but little data exists as many rely on informal channels to send money home. Today's African diaspora consists of approximately 20 to 30 million adults, who send billions annually to their families and local communities back home. For the region as a whole, this represents 50% more than net Official Development Assistance (ODA) from all sources, and, for most countries, the amount also exceeds Foreign Direct Investment (FDI). In several fragile states, remittances are estimated to exceed 50% of GDP. Most African countries restrict the payment of remittances to banks, which in turn, typically enter into exclusive arrangements with large money transfer companies, like Western Union or Money Gram, to operate on their behalf. This results in limited competition and limited access for consumers, although there are a number of new players aiming to disrupt this established Money Transfer Operator (MTO) model, such as Xoom and Willstream, which leverage increasing mobile phone penetration in the region and provide different rate structures to diaspora customers. The World Bank though noted that “Cross-border mobile remittances have not taken off due to a variety of regulatory and operational challenges with mobile remittances falling into a regulatory void between financial and telecom regulations which creates regulatory uncertainty for potential market entrants”. According to a World Bank study, Nigeria is by far the top remittance recipient in Africa, accounting for US\$10bio in 2010, a slight increase over the previous year (US\$9.6bio). Other top recipients include Sudan (US\$3.2bio), Kenya (US\$1.8bio), Senegal (US\$1.2bio), South Africa (US\$1.0bio), Uganda (US\$0.8bio), Lesotho (US\$0.5bio), Ethiopia (US\$387miln), Mali (US\$385mio), and Togo (US\$302mio). As a share of GDP, the top recipients in 2009 were: Lesotho (25%), Togo (10%), Cape Verde (9%), Guinea-Bissau (9%), Senegal (9%), Gambia (8%), Liberia (6%), Sudan (6%), Nigeria (6%), and Kenya (5%).

Since 9/11, the FATF and member countries have taken steps to address the risks of MSB and informal value transfer systems.

The internationally co-ordinated effort to address money laundering and terrorist financing has likely increased the cost of sending remittances, which in turn has likely increased the amount of remittances sent through informal channels (family connections, travelling friends, local money lenders etc.).

Definition/Description

MSBs are non-bank entities which provide transfer and exchange mechanisms. People generally use MSBs to exchange or transfer value, or to purchase or redeem negotiable instruments. Depending on the jurisdiction, a MSB may be defined as an individual or an entity that is engaged in the business of any of the following activities:

- foreign exchange dealing;
- remitting or transmitting funds by any means or through any individual, entity or electronic funds transfer network; and/or
- issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments.

MSBs are sometimes known as Casa de Cambio, Exchange Houses, Cheque Cashers, Money Transmitters, Currency Dealers, etc. and can include unregulated or informal MSBs or alternative remittance systems (ARS) such as hawala, hundi, undiyal, fei ch'ien, chitti, or other informal value transfer systems.

Money Laundering/Terrorist Financing Risks

MSBs provide a range of unique, valuable, and competitive financial services for domestic and international customers, and while the variety of MSB types and sizes can provide consumers with expanded choices, it also means that the sector has unique challenges and risks and have shown themselves especially vulnerable to misuse for money laundering and terrorist financing.

Particular concerns exist around the use of MSBs by organised crime and in particularly drug traffickers in Latin America to launder drug money as well as tax fraudsters and evaders and terrorist groups to move money.

Since the mid-1990s, US bank regulators and drug enforcement investigators have been warning that Mexican MSBs in particular, Casas de Cambio pose a significant money laundering risk. Casas de Cambio allow people and businesses for example in Mexico to exchange or wire transfer the value of currency to bank accounts in the US and other countries, via accounts they hold with banks (see Correspondent Banking in Part 1, Section 2, Sub-section 3, Products and Services Risks below). The Casas de Cambio in Mexico, and elsewhere in Latin America, are notorious for dealing and involvement with funds from and to drug traffickers which are then processed via correspondent accounts at US or foreign banks. It is unsurprising that Casas are involved as so much of the Mexican economy is connected with organised crime and drug trafficking, and the risks as such may also exist therefore with other

financial services businesses including banks in Mexico

Common techniques most illustrative of how MSBs can be exploited for money laundering and terrorist financing purposes include structuring and attempting to circumvent MSB record keeping requirements that would disclose the MSB client's identity; attempting to circumvent MSB identification requirements; smurfing, using nominees, or other proxies; exploiting negotiable instruments such as money order and bank cheques; and refining small bills into larger transactions.

A Casa de Cambio is an exchange house operating extensively throughout Mexico and in the US on the US/Mexican border. The US government has warned that Casa de Cambios are commonly used by money launderers. A Casa de Cambio in the US may collect several transmittal orders for small amounts from different individuals wanting to send money to relatives in Mexico. The Casa de Cambio then bundles them into a single transmittal order to a US bank as part of a transmittal of funds to a Mexican Casa de Cambio. The single transmittal order does not identify all transmitters or recipients of the underlying order. The US bank simply sends the single transmittal order to the Mexican bank which then pays the Mexican Casa de Cambio which then pays the Mexican recipients based on the separate transmittal orders received directly from the US Casa de Cambio. See Part 2, Section 7 Pedro Allatore and Casa de Cambio Pueblo, Beacon Hill and Lespan and Part 2, Section 8 , HSBC, Wachovia and Sigue Corp, all of which led to enforcement actions against the financial institutions.

Another area of particular money laundering and terrorist financing risk involves Unregulated Money Service Businesses.

Unregulated Money Service Businesses (UMSB)

UMSBs are any entity which is engaged in the business of a money services business but which is not properly licensed, regulated and as such is not required to operate an AML Programme.

Examples of UMSBs can include unregistered ARS sometimes known as integrant banking, informal funds transfer systems, hawala (Islamic countries), hundi (India), undiyal, fei ch'ien (China), chitti and Black Market Peso Exchange (South America), Chop (China), or other informal value transfer systems (IVTS). For a variety of socio-cultural and economic reasons, ARS are pervasive in many parts of the world. ARS provide a cost-effective means of moving money, particularly in those parts of the world which have little or no formal banking infrastructure. Since ARS usually operate on

the basis of trust between remitters (and intermediaries acting on their behalf), they are able to persist outside of the normal financial system and avoid regulatory controls, and may not record clients and transactions in the way that registered MSBs must do. As useful as ARS may be to a wide variety of financial services consumers, a number of jurisdictions and international bodies have identified ML/TF risks linked to the possibility of anonymity which ARS can provide, and in relation to risks associated with the lack of recordkeeping and absence of report filing. Unregistered MSBs and ARS systems do not submit mandatory transaction reporting and create opportunities for anonymity within the financial system. These issues could create AML/CTF vulnerabilities and also create investigative obstacles. Unregistered remittance businesses should also be a concern for the MSB sector in that these operations can create reputational risks for registered MSBs and other financial institutions which may ultimately be used (knowingly or not) as settlement mechanisms for an unregistered remitter who could potentially be facilitating illicit financial activity. The most common point of contact between a UMSB and formal sectors lies in the bilateral or multilateral process of financial settlement of debts with other dealers/operators incurred as a result of the trust-based transactions common to these remittance systems.

Increasingly, UMSBs are evolving from store front operations where customers drop off cash to e-currency, digital businesses where remitting party and beneficiary are completely opaque, with customers engaging with a decentralised host with no obvious domicile or location.

FATF released a typology on ARS in 2005 and developed the Special Recommendation VI now Recommendation 14 in response.

Chop

Chop is a Chinese alternative remittance system. It works the same way as the Hawala system, but while Hawala is more based on trust and the extensive use of ethnic or familial connections, the Chop system relies on chops. The broker creates a chop, tears it into two pieces and gives one piece to the client and sends the other piece to his counterpart broker in the other country. The client sends his half of the chop to the recipient and the match of the two halves will provide evidence to the broker to release the money to the recipient.

Fei ch'ien

Fei Ch'ien a Chinese ARS and means flying money or coin. The system to transfer funds including tax revenues evolved during the latter half of the T'ang

Dynasty as a result of the growing commodity trade within China. Merchants from the southern part of China sold goods in the capital and transferred their revenues from the sales to agencies of their provinces where these revenues were used to pay taxes. These agencies issued certificates indicating the amounts paid by the merchants who would after their return present them to the provincial governments for payment of an equivalent sum of money. Through these transfers the merchants and couriers of the provincial governments could avoid the inconvenience and risk involved in transporting money physically over long distances. With the Chinese emigration in the 19th century the system became internationalised by the flow of remittances from the expatriates in order to support their families that stayed in China.

Hawala

Hawala is an ancient system for remitting money primarily in Islamic societies. Clients entrust money to hawala bankers who facilitate money movement worldwide through personal connections, sometimes using legitimate bank accounts, but leaving minimal paper trail which makes it easy for the hawaladars and their clients to avoid legal repercussions. The hawala triangle (Dubai, India and Pakistan) is responsible for the heaviest traffic in worldwide financial transfers. Hawala provides a fast and cost-effective method for worldwide remittance of money or value particularly in regions outside the reach of the financial sector. Since hawala payments provide security, anonymity and versatility to the user, the system can be easily misused for money laundering, terrorist financing and other financial crimes. However, in some countries they operate in parallel with formal financial institutions or as a substitute or alternative for them.

Hundi

Hundi is an alternative remittance system which works the same way as a hawala system but evolved in the Indian subcontinent and was spread to neighbouring countries. It used to be one of the main payment method in India even up to the 1960s.

For details about the Black Market Peso Exchange see Part 1, Section 1, Drug Trafficking; and about Cash Smuggling see Part 1, Section 1, Smuggling.

Politically Exposed Persons

"Power tends to corrupt, and absolute power corrupts absolutely. Great men are almost always bad men."

John Emerich Edward Dalberg Acton, Lord Acton, British historian and moralist 1887²⁵

Introduction

Public officials, particularly ones who attain important public positions and acquire power over their citizens as a result are neither innately bad nor corrupt. Most begin as honest men and women with honourable, patriotic, and even altruistic motives, wishing "to do good for the people" but the longer the time in power and the more senior the position held, it would seem the more likely the person is to succumb to weaknesses in morality, and to abuse the position of public trust to which they have risen.

Whilst not all senior public officials seek to attain and establish themselves in the way of absolute monarchies from antiquity and through the middle ages, where all power is given to, or, as is more often the case, taken by, the monarch, for example, Roman emperors (who declared themselves gods), Catholic Popes (Gods' chosen priest on earth), and Napoleon Bonaparte (who declared himself an emperor and above God!), some still remain and others still aspire to such heights. The more common abuse is the President, Prime or Senior Minister who increasingly over time becomes more abusive, placing restrictions on human rights, increasingly using force against the people, and surrounding himself with family members and cronies, appointing friends and supporters to lucrative positions or awarding them lucrative contracts, diverting public funds or foreign aid for grandiose projects or private enrichment. If there is meaningful opposition, an emergency may be declared or created to justify police or military action. Once a ruler is in power for long enough he will eventually confuse state assets for his own and no longer be accountable for his actions and will do what is politically and personally expedient. A prime example is the case of Sani Abacha who was President of Nigeria between 1993 and 1998. He was listed in 2004 by Transparency International as the fourth most corrupt leader of all time, with an estimated theft of state assets of at least US\$2-5bio. The term Politically Exposed Person (PEP) was indeed a term coined as a result of the Abacha case. The sheer size of the assets involved and the number of financial institutions involved across many major financial centres directly led to a re-evaluation and a recognition that

anti-money laundering controls in financial institutions needed to be enhanced.

Definition/Description

The Abacha case led at least to one government, in this case the Swiss Government, to react and to issue a directive to its banks in 1998 that first used the phrase Politically Exposed Persons. This was taken up by the Wolfsberg Group which joined together to issue their first statement covering private banking principles, covering expressly how to manage PEP relationships in 2000, leading to inclusion in a 2001 paper of the Basel Committee on Banking Supervision and then being formally adopted by FATF as a special category in 2003. Consequently, there are numerous definitions of PEP though many share the same characteristics. A Politically Exposed Person is a natural person who performs (or has performed) a prominent/important/senior, foreign public position. This definition includes anyone who is identified as being a close family member of, or closely associated with such an individual.²⁶

Money Laundering/Terrorist Financing Risks

Over the past 25 years, we have learned about the plunder of state assets by PEPs with TI listing in 2004 their most corrupt top 10 PEPs as follows:

Top 10 most corrupt leaders (as at 2004)			
No	Name	Country/Period	Amounts
1	Mohamed Suharto	Indonesia: 1867-1998	US\$15-35bio
2	Ferdinand Marcos	Philippines: 1972-1986	US\$5-10bio
3	Mobutu Sese Seko	Zaire: 1965-1997	US\$5bio
4	Sani Abacha	Nigeria: 1993-1998	US\$2-5bio
5	Slobodan Milosevic	Serbia/Yugo: 1989-2000	US\$1bio
6	Jean-Claude Duvalier	Haiti: 1971-1986	US\$300-800mio
7	Alberto Fujimori	Peru: 1990-2000	US\$600mio
8	Pavlo Lazarenko	Ukraine: 1996-1997	US\$114-200mio
9	Arnoldo Aleman	Nicaragua: 1997-2002	US\$100mio
10	Joseph Estrada	Philippines: 1998-2001	US\$78-80mio

Source: Transparency International 2004²⁷

Whilst these PEPs fall into the category generally known as kleptocrats, corruption risks are not the only risks presented by PEPs. These PEPs were likely also involved in murder, kidnap and human rights abuses alongside. PEPs like General Augusto Pinochet of Chile may have been involved in drug trafficking and other organised criminal activities either directly, for example in the case of General Manuel Noriega in Panama, or indirectly in the case of Raúl Salinas, the brother of then President Carlos Salinas of Mexico. PEPs may also be involved in financing terrorism, which would certainly include Colonel Muammar Gaddafi of Libya, and Weapons of Mass Destruction Proliferation, for example at least at some stage by President Saddam Hussein of Iraq and Kim Jung Il of North Korea who also pursued currency counterfeiting as a means of generating illegal profits.

Nevertheless it is in the area of corruption that senior public officials are most exposed and on occasions some will become corrupt and then some will engage in grand corruption on a massive scale. Whilst corrupt PEPs are probably a small portion of the entire population of PEPs, a single corrupt PEP can have a significant impact on a country and on a region.

The ways in which corrupt PEPs laundered their corrupt monies have a classic and familiar feel. Corrupt heads of state and prominent public officials would open bank accounts in their own names in foreign offshore centres or use relatives to open and operate bank accounts. They may well open numerous accounts at different banks in different centres to both diversify their risks and also to ensure no one but themselves could appreciate the true picture of the total wealth accumulated. The classic case is likely no longer as viable as foreign governments once supportive of corrupt regimes as a bulwark against the spread of an alternative political philosophy or regional instability, even financing them indirectly through commodity business, inward investment and aid, have adopted a more critical stance, law enforcement and regulators have become serious about compliance with new improved standards and banks have largely stepped up their approach when dealing with PEPs. Also the emergence of NGOs like Transparency International, Basel Institute of Governance and Global Witness seek to ensure civil society hold stakeholders to account.

More recent techniques show that PEPs continue to include the use and abuse of bank facilities but this is done by using close associates as fronts or cover for the PEP and/or by the use of intermediaries, and/or gatekeepers to establish complex and opaque corporate structures in order to hide the involvement or interest of the PEP. PEPs will also in addition to retaining some assets in bank accounts, diversify into holding

physical cash or negotiable securities, acquiring physical property, for example real estate, precious metals and stones, and high value goods, such as art, cars, planes and boats.

Whilst the conversion of corrupt monies into assets may assist a PEP in avoiding holding large sums in bank accounts where such assets are under greater scrutiny, such assets may not avoid the glare of publicity which the corrupt PEP will want to avoid.

Whilst close associates certainly continue to benefit from ties to corrupt PEPs more modern techniques will not have the close associate holding assets as a strawman for a corrupt PEP but the close associate will instead benefit through contracts and concessions awarded and allowed to prosper by the PEP who then builds a successful business and either provides every comfort to the PEP during his tenure or provides for his retirement after he leaves office.

A variation on this, and it must be said in this case there is no suggestion of illegality, perhaps however illustrates the point in the modern context of how even in the heart of Europe, PEPs may be perceived as benefiting from their public office and how the challenges for identifying PEPs misuse of power for private gain may develop. Gerhard Schröder was German Chancellor from 1998 until 2005 and was a strong advocate of the Nord Stream pipeline project, which aimed to supply Russian gas directly to Germany, bypassing transit countries, who would have been able to charge for the privilege and would have provided them some influence over the Russians. Nevertheless, the agreement to build the pipeline was signed two weeks before the German elections, just a few weeks before Schröder stepped down as Chancellor. Soon after stepping down as chancellor, Schröder accepted Gazprom's nomination for the lucrative post of the head of the shareholders' committee of Nord Stream AG. German opposition parties expressed concern over the issue, as did the governments of countries over whose territory gas was already being pumped. In January 2009, Schröder also agreed to join the board of the oil company TNK-BP, a joint venture between oil major BP and Russian partners. Gerhard Schröder was not the first and many more PEPs have benefited handsomely from their time in office after stepping down, many like Schröder no doubt legally, others not so.

Chancellor Schröder is not the only PEP to find substantial rewards awaiting him after he leaves office, though the trend appears to be a noticeable one.

Sovereign Wealth Funds

Given the sums of monies managed and/or at the disposal of Sovereign Wealth Funds (SWF), the opportunity for corruption and bribery is high. Such is the perceived risk that in 2008 the Chief of the Fraud Section at the US Department of Justice, Steve Tyrell, said the "recent boom of sovereign wealth funds is an area at the top of the Justice Department's hit list". In 2011 a reported inquiry into certain Financial Institutions dealings with sovereign wealth funds, was announced. While no allegations of any wrong doing was reported, the SEC nonetheless requested information from a targeted group of US based financial institutions. The probe was essentially into possible violations of the primary US anti-corruption legislation, Foreign Corrupt Practices Act ("FCPA"), in connection with investments made by Sovereign Wealth Funds just before or during the global financial crisis of 2008. See Part 2, Section 8, Outlook Cases below.

No	Top 20 Sovereign Wealth Funds	Assets US\$bio
1	UAE-Abu Dhabi Inv Authority	627
2	Norway Gov Pension Fund - Global	593
3	China SAFE Investment Co	567.9**
4	Saudi Arabia SAMA Foreign Hldgs	532.8
5	China Investment Corp	482
6	Kuwait Investment Authority	296
7	China-HK MA Investment Portfolio	293.30
8	Singapore Investment Corp	247.5
9	Singapore Temasek Holdings	157.5
10	Russia National Welfare Fund	149.7*
11	China National Social Security Fund	134.5
12	Qatar Investment Authority	100
13	Australian Future Fund	80
14	UAE-Dubai Investment	70
15	UAE-Abu Dhabi Inter Pet Inv Co	65.3
16	Libyan Investment Authority	65
17	Kazakhstan National Fund	58.2
18	Algeria Revenue Regulation Fund	56.7
19	UAE-Abu Dhabi Mubadala Development Co	48.2
20	South Korean Inv Corp	43

Source: <http://www.swfinstitute.org/fund-rankings/>

*This includes the oil stabilization fund of Russia.

**This number is a best guess estimation.

The finances available to these funds make them an attractive source of revenues for many institutions such as asset managers, investment banks, and custodians to name a few. This potential revenue may encourage misguided professionals and those who are prepared to engage in unethical business practices to target SWFs. The risks that apply to SWFs may also equally apply to other government funds and assets.

SWFs are increasingly playing an important role in the global economy and the international financial system. Assets under management of SWFs are currently estimated to total US\$2-3 trillion, exceeding assets managed by hedge funds (US\$2.3 trillion). These funds' assets are projected to surpass global foreign exchange reserves and are forecasted to exceed US\$7-11 trillion by beyond 2013.

Generally SWFs fall into two categories: commodities funds, financed by commodity exports (such as oil) and non-commodity funds, which are usually financed by excess of foreign current reserves.

The International Monetary Fund highlights that typically SWFs can be categorised as stabilisation funds, savings funds, pension reserve funds, or reserve investment corporations. The majority of these funds are savings funds for future generations or fiscal stabilisation funds. Examples of reserve investment corporations include for example, China Investment Corporation (CIC), Korea Investment Corporation (KIC), and Government Investment Corporation of Singapore (GIC). The top 20 Sovereign Wealth Funds as compiled by the SWF institute 2008 are listed above:

Public finance management is always susceptible to abuse and SWFs are no exception, though most are generally well run and should be of little concern. Still, the funds have different legal structures, governance and levels of transparency, which are often reflective of the economic and regulatory development of the state itself.

Precious Metals & Stones Dealers

"A diamond is forever"
De Beers Marketing

Introduction

These precious stones alongside others and precious metals, whilst highly sought after by many for legitimate reasons are attractive to criminals in many ways. Historically, precious metals were important as a currency but are now regarded mainly as an investment and as industrial commodities.

In addition to their long association with money, precious metals and stones have a similarly long association with crime due to their equivalency to money and the fact that they are easily transportable, concentrated forms of wealth that can be exchanged for cash anywhere in the world. In addition, precious metals, especially gold, silver, and platinum, have a ready, actively traded market, and can be melted and poured into various forms, thereby erasing refinery marks while precious stones have usually no markings especially rough stones leaving them untraceable. For these reasons, precious metals and stones are highly attractive to money launderers and other criminals, including those involved in the financing of terrorism.

Dealers in these precious products and financial institutions that conduct business relationships with dealers should be wary of the potential involvement in criminal activity for the purpose of money laundering or terrorist financing.

Dealers could include a wide range of persons, from those who produce precious metals or precious stones at mining operations, to intermediate buyers and brokers, to precious stone cutters and polishers and precious metal refiners, to jewellery manufacturers who use precious metals and precious stones, to retail sellers to the public, to buyers and sellers in the secondary and scrap markets. Still those that only manufacture jewellery or are only involved in mining, cutting or polishing may be excluded from the dealer definition.

Definition/Description

FATF have identified a class of businesses they call, "Designated Non-Financial Professions and Businesses (DNFPBs)" being professions and businesses that are seen as being attractive to money launderers and these are: casinos, (when their customers engage in financial transactions above US\$/€3,000), lawyers, accountants

and trust and company service providers, dealers in precious metals and stones (when their customers engage in cash transactions above US\$/€15,000) and real estate agents. As far as precious metals and stones are concerned, the regulations typically exclude businesses where the purchases or sales are carried out for, connected with, or for the purpose of manufacturing jewellery or extracting precious metals from a mine.

A precious metal is a rare, naturally occurring metallic chemical element of high economic value. The status of a "precious" metal can also be determined by high demand or market value. Precious metals in bulk form are known as bullion and are traded on commodity markets. Bullion metals may be cast into ingots or minted into coins. The defining attribute of bullion is that it is valued by its mass and purity rather than by face value as in the case of money. Chemically, the precious metals are less reactive than most elements and have a shiny surface. Gold, silver, platinum, and palladium are considered the four principal precious metals.

Whilst gold and silver were used extensively in coinage, art and jewellery, platinum has only relatively recently acquired both its place in jewellery and investment portfolios, since being discovered during the Spanish conquest of the New World. Palladium is mostly used in catalytic converters, which convert harmful gases from car exhausts into less-harmful substances, and is also used in electronics, dentistry, medicine, hydrogen purification, chemical applications, and groundwater treatment. Palladium plays a key role in the technology used for fuel cells, which combine hydrogen and oxygen to produce electricity, heat, and water.

The demand for precious metals is driven not only by their practical use but also by their role as investments and a store of value. Historically, precious metals have commanded much higher prices than common industrial metals.

Gold and silver, and sometimes other precious metals, are often seen as hedges against both inflation and economic downturn. Silver coins have become popular with collectors due to their relative affordability, and, unlike most gold and platinum issues which are valued based upon the markets, silver issues are more often valued as collectables, far higher than their actual bullion value.

Money Laundering/ Terrorist Financing Risks

Precious Stones are today considered to include only four, namely the diamond, ruby, sapphire and emerald

which traditionally command a premium price in the market due to their extraordinary colour or brilliance and extreme rarity. Historically speaking other stones were considered as "precious", though now they are more properly considered "semi-precious" and include, pearl, though not strictly speaking a gemstone, opal and amethyst. Other less well known and rarer so called "semi-precious" stones such as alexandrite, demantoid garnet, tsavorite garnet and tanzanite can be just as expensive as a ruby or sapphire. Very fine tourmaline, spinel and aquamarine in larger sizes also command very high prices in the market, so the difference between precious and semi precious may need to be revised.

Of all the precious stones, diamond is the most popular and generally the most expensive, but interestingly is no longer particularly rare. After the discovery of huge South African diamond finds in 1870, diamonds could be mined by the ton. There was such a glut of supply and so little demand that the British financiers of the South African mines were in danger of losing their investment. Their solution was to create the powerful De Beers cartel that to this day controls worldwide diamond production and supply. Quality diamonds are actually not scarce at all. But De Beers controls how much supply comes on to the market and that keeps prices high. The De Beers consortium also mounted a concerted decades-long advertising campaign to associate diamonds with love, courtship and marriage, under the now familiar slogan "A diamond is forever".

The diamond engagement ring, once unknown in most parts of the world (including Europe), is now considered an essential part of the ritual of marriage. It is hard to avoid the conclusion that diamond's special position as a precious stone is due largely to monopoly economics, and clever marketing.

Precious stones, jewels and precious metals have unique physical and commercial properties which carry value in small, easily transportable quantities and are forms of wealth that can be exchanged for cash anywhere in the world.

Some of the most exquisite come in the form of jewellery and command great prices too. The most expensive jewellery include, tiaras to rings, being purchased at auction with the most expensive, a pink round-cornered rectangular diamond purchased by famed jeweler Laurence Graff for US\$46.2mio. The diamond was formerly owned by jeweller Harry Winston. This beauty set the record for most expensive single jewel ever sold at auction. Laurence Graff renamed it "The Graff Pink."

Top 5 precious stone jewels sold at auction		
1	The Graff Pink	US\$46.2mio
2	The Wittelsbach-Graff Diamond	US\$24.3mio
3	The Perfect Pink	US\$23.2mio
4	Bulgari two-stone coloured Diamond & Diamond Ring	US\$15.7mio
5	Wallis Simpson's Panther Bracelet	US\$12.4mio

Source: Author

In addition, precious metals, especially gold, silver, and platinum have a ready, actively traded market, and can be melted and poured into various forms, thereby erasing refinery marks and leaving them untraceable.

Gold, for example, is a major precious metal commodity that poses risk for the following reasons: it has a high intrinsic value that can be authenticated; it is not subject to issuer risk, and; it is easily convertible (exchangeable), can be transported and fabricated. Gold is sourced from the ground by mining companies who produce approximately 65% of the annual total with recycled gold contributing to the rest of the annual supply. The recycling of gold ensures there is a potential source of readily available supply when needed. This helps to cater for an increase in demand and keep the gold price stable. On the demand side jewellery production accounts for almost half with bar and coin demand slightly behind.

Gold production and reserves by Country (2007)		
1	China	11.3%
2	South Africa	11%
3	Australia	11%
4	US	10%
5	Peru	7%
6	Russia	7%
7	Indonesia	6%
8	Canada	4%
9	Others	34%

Source: Minerals Resources Programme of the US Geological Survey (Mineral Commodities Summary, 2010)

The other precious metals; silver, palladium, and platinum do not exhibit the same high risks as gold. For

example, using July 2010 prices, silver which is priced at US\$588/kg, compared to platinum at US\$87,741/kg and gold at US\$24,317/kg, is hardly a precious metal at all and has low consumption levels. Silver and palladium (US\$13,632/kg) are also hardly used in the jewellery business, but more in industry which is substantially less prone to money laundering risks.

Digital Precious Metals

Digital precious metals, a relatively new way of transferring value online, enable users to secure cash deposits against precious metals held offshore. A recent report published by US National Drug Intelligence Centre (US NDIC) observed that digital gold currencies are the most popular type of digital currency. According to the Global Digital Currency Association (GDCA), digital currency transactions account for billions of dollars each year. Digital gold currency transactions alone increased from approximately US\$3bio in 2004 to approximately US\$10bio in 2006. For details on e-gold, an electronic currency reportedly backed by gold bullion see Part 2, Section 7, Criminal Cases, [Douglas Jackson](#). Individuals establish online accounts by providing their names, e-mail addresses and physical addresses which can be easily fabricated and a valid e-mail address. Some digital precious metals also allow users to establish anonymous accounts. Once the accounts are established, individuals can then trade their virtual holdings of precious metals with account holders (or with other accounts held by the same beneficial owner in the case of money laundering). US NDIC also noted that in some digital currency services, anonymity continues during the digital currency account funding process. Individuals can fund digital currency accounts by making cash deposits directly to an exchanger's bank account. The seller transfers ownership of the virtual precious metal holdings to the purchaser at the completion of a transaction. The proceeds can be received through a variety of traditional and non-traditional payment methods. Digital precious metals may also be used to purchase goods and services at participating merchants or be redeemed into physical gold.

A case where digital precious metals such as e-gold were abused involved the arrest of the members of the organised cybercriminal group, Shadowcrew. In October 2004, the US Secret Service closed an illegal online website that trafficked in at least 1.5 million stolen credit and bank card numbers that resulted in losses in excess of US\$4mio. It was alleged that payments for illicit merchandise and services was paid for and received by Shadowcrew members using systems including e-gold and Web Money. Six Shadowcrew members were eventually charged with conspiracy to commit credit

and bank card fraud, as well as identification document fraud. One of the six defendants was also charged with the unlawful transfer of identification documents to facilitate criminal conduct. Several others were indicted on conspiracy charges. In June 2006, the alleged ringleader was sentenced to 32 months imprisonment.

More recently interest and concern has risen regarding "Bitcoin" which is now 5 years old and has become the flagship of digital currencies, though heads a long list including: Copperlark, Feathercoin, Litecoin, Megacoin, Mincoin, Namecoin, Novacoin, Peercoin, Phenixcoin, Primecoin, Protoshares, Quarkcoin, Terracoin and Worldcoin.²⁸

"Conflict Diamonds" or "Blood Diamonds"

A major concern has arisen which deserves particular mention, namely Conflict or Blood Diamonds.

Conflict diamonds or also known as blood diamonds are diamonds that are used to fuel violent conflict and human rights abuses. They have funded brutal wars in Africa, in particular in Angola, Liberia, Sierra Leone, Democratic Republic of Congo and the Ivory Coast that have resulted in the death and displacement of millions of people. Diamonds have also been used by terrorist groups such as [Al-Qaeda](#) to finance their activities and for money laundering purposes.

Reports estimated that as much as 20% of the total diamond production in the 1980s was being sold for illegal purposes and 19% was specifically conflict in nature. By 1999, the illegal diamond trade was estimated by the World Diamond Council to have been reduced to 3.06% of the world's diamond production. The World Diamond Council reported that by 2004 this percentage had fallen to approximately 1%.

Angola

During the decades long (1974–2001) Angolan Civil War, the [National Union for the Total Independence of Angola \(UNITA\)](#), financed its war with the Government by selling Angolan diamonds, valued at up to US\$3.7bio over the period.²⁹

The UN recognised the role that diamonds played in funding the [UNITA](#) rebels and in 1998 passed UN Security Council Resolutions 1173 and 1176, banning the purchase of conflict diamonds from Angola. Despite the UN Resolution, [UNITA](#) was able to continue to sell or barter some diamonds in order to finance its war effort. As a result a global initiative was undertaken that culminated in the Kimberley Process Certification Scheme (see below for details).

Liberia and Sierra Leone

From 1989 to 2003, Liberia was engaged in a civil war. In 2000, the UN accused Liberian President Charles Taylor of supporting the [Revolutionary United Front \(RUF\)](#) insurgency in neighbouring Sierra Leone with weapons and training. To finance the weapons purchases and support, the [RUF](#) provided Charles Taylor with Sierra Leone diamonds.

In 2001, the UN applied sanctions on this conflict diamond trade, which has since been lifted. In August 2003, Charles Taylor stepped down as President and, after being exiled to Nigeria, was extradited and faced trial in The Hague, being found guilty in 2012 of crimes against humanity and war crimes, he is now serving a 50 year sentence in a high security prison in the UK.

It has also been reported that around the time of the [1998 US Embassy bombings in East Africa](#), [Al-Qaeda](#) bought diamonds from the [RUF](#) in Liberia, converting their cash assets into diamonds.

Ivory Coast

Following a coup in 1999 and resulting Civil War, diamonds from Liberia and from Sierra Leone in addition to locally mined diamonds were trafficked through the country and funds derived from this trade used to support those involved in the Civil War. To curtail the illegal trade, the Government stopped all diamond mining and the UN Security Council banned all exports of diamonds from Côte d'Ivoire in December 2005. Despite UN sanctions, however, the illicit diamond trade still exists in Côte d'Ivoire. Rough diamonds are exported out of the country to neighboring states and then on to international trading centres, through the northern controlled section of the country where rebel forces are reported to be using these funds to re-arm.

Democratic Republic of the Congo

The Democratic Republic of the Congo (DRC and formerly Zaire) has suffered numerous civil wars in the 1990s, but now is relatively stable, though the prospect of conflict especially around election time is a recurring risk. The abundant minerals and jewels that can be found in the DRC provided both a basis for past conflict but also the means to forge agreements and establish peace amongst the various groups vying for power in the DRC.

The DRC exports about 8% of the world's diamonds, with one of the most celebrated and priceless diamonds, the "Star", a flawless D-colour 200 carats (40g) being discovered in the DRC and sold during a past civil war in the early 1990s to De Beers.

In addition to diamonds, DRC has also had experiences of the illicit trade in particular valuable minerals, including cassiterite, (the ore for tin), coltan (the ore for a rare metal called tantalum), wolframite (tungsten ore), and gold. The illicit trade provided rebel groups and units of the national army with tens of millions of dollars a year that are then used to finance arms purchases and campaign finance or voter fraud at election time.

Claims that Congolese diamonds are sought and bought by terrorist groups are difficult to prove, but allegations are made.³⁰

The Republic of Congo

The Republic of Congo (Congo-Brazzaville) was up until 2004–2007 exporting large quantities of diamonds, most likely shipped from the DRC and was also accused of falsifying certificates of origin. It has since improved its approach to diamonds and has tried to clean up its image.

Zimbabwe

Zimbabwean diamonds are not officially considered conflict diamonds, but NGOs like Global Witness³¹ claim that exports from companies operating in the controversial "Marange" diamond fields in Zimbabwe are tainted. They claim that the Zimbabwean army effectively seized control of the area in 2008, killing around 200 miners. Mining concessions were then granted in legally questionable circumstances to several companies, some of them associated with senior figures in Robert Mugabe's Zanu PF party. Newspapers have reported that the Zimbabwean Central Intelligence Organisation, the state security service aligned with Mugabe whose members are accused of committing acts of violence against opposition supporters, directly benefits from off-budget diamond revenues. Again according to Global Witness, "Over the last decade, elections in Zimbabwe have been associated with the brutal intimidation of voters. Orchestrating this kind of violence costs a lot of money. As the country approaches another election there is a very high risk of Zanu PF hardliners employing these tactics once more and using Marange diamonds to foot the bill."

Kimberley Process Certification Scheme (KPCS)³²

In 2000, the World Diamond Congress (now World Diamond Council) adopted at Antwerp a resolution to strengthen the diamond industry's ability to block sales of conflict diamonds, and in 2002 the UN approved the results. Whilst initially supported the process is losing support internationally such that it is beginning to be seen as seriously compromised and weakened.

Private Military Firms

"Although some might argue that it is a peculiarly male version of prostitution, it has effectively been around for as long as war has been waged."

by Peter Tickler in 'The Modern Mercenary'

Introduction

Private Military Firms (PMFs) have been in the national and international spotlight in recent years, most famously known are the actions of some in Iraq. There are many mixed feelings about PMFs, some say that they are necessary and that they help countries to save money, but to others, they threaten the role of the state in overseeing its armed forces, by gathering intelligence, supplying forces and building influence they profit from war, pose risks of corruption and may be likely to encourage military action abroad.

Definition/Description

A private military firm (PMF) is a private sector entity that provides services that are intricately linked to warfare. One of the leading researchers on the topic, Peter W. Singer of the Brookings Institution,³³ distinguishes three types of PMFs:

- i) Military Provider Firms (MPF) providing direct tactical, military assistance which may include front-line combat;
- ii) Military Consultant Firms (MCF) providing expert strategic advisory & training services; and
- iii) Military Support Firms (MSF) providing logistics, intelligence and maintenance services.

MPFs frequently provide military-style security, labelling this as defensive or passive work. Yet in this role they can quickly find themselves in a battle that puts them in the role of actual, or perceived, aggressor. An example of an MCF is a subsidiary of a western arms manufacturer, providing training for equipment it sold to another Western state in that same state. Another example is a company providing training to foreign police forces. An example of a MSF is a consultancy analysing satellite imagery for the military, or a company running the canteens for an army base. MCFs and MSFs can work both in peaceful environments, battlefields or in otherwise corrupt or unstable environments.

Money Laundering/Terrorism Financing Risks

The PMF industry has displayed strong growth in the past few years. Even before the Iraq War, it was estimated that the industry had annual market revenue in the range of US\$100bio which would at least double

by 2010. Large contracts are awarded for example by governments for logistics services to their militaries, by the private sector for military-style protection of personnel and facilities, and by international organisations for humanitarian de-mining operations. With the Iraq War, the market exploded. It is estimated that about 181 private firms with around close to 50'000 armed employees carried out military functions in Iraq. The US State Department spent for example US\$500mio in 2008 on PMFs.³⁴

PMFs have made negative headlines, though they have also provided some heroic and valuable services. The risks associated with PMFs are, however, not new as PMFs in many instances have men operating in corrupt and unstable environments. The principals often cannot fully verify whether the billed services correspond to the services actually provided. Many payments are made in cash. The risk of corruption and fraud, and therefore money laundering, is high. As there is so much money to be made, profiteering cannot be ignored and in a war zone, there is little enough good governance, transparency or accountability.

The industry is also controversial because PMFs are rarely sanctioned or fully investigated when allegations of misbehaviour surface. Even if major crimes are done, PMF's may enjoy significant protection. In passing the Coalition Provisional Authority Order 17 of June 2003, for example, the provisional Iraqi Government granted exemption from prosecution to all personnel action on behalf of the coalition including PMF employees. Critics also point to outsourcing military tasks not for effectiveness but to "improve" figures on troop numbers and body counts. Further, there is the risk that states that outsource military functions run the risk of increasing dependency which is financially detrimental and not conducive to the rapid resolution of the conflict situation at hand.

During the Iraq occupation, tens of thousands of PMFs worked alongside the regular military soldier. Perhaps the most well known was Blackwater USA (renamed Xe Services and now Academi) who provided services ranging from feeding the troops to armed combat. According to P. W. Singer, the author of *Corporate Warriors: The Rise of the Privatized Military Industry*,³⁵ their pay ranged from US\$250 a month for Kurdish fighters to US\$1,000 a day for former US Green Berets. One example in Iraq in 2004 highlights the problems. Blackwater employees entered the city of Fallujah, looking apparently for terrorists, but according to others in fact spent their time, carrying out night-time raids, assaulting women and children, and torturing and murdering local men and teenage boys.

Major Private Military Firms		
No	Name	Country
1	G4S	UK
2	Unity Resources	Aus
3	Erinys	US
4	Asia Security Group	Afghanistan
5	DynCorp	US
6	Triple Canopy	US
7	Aegis Defence Services	UK
8	Defion International	Peru
9	Academi (formerly Blackwater / Xe Services)	US

Source: BusinessInsider.com

mercenary group for hire that was disbanded in 1998, though retained contacts with Simon Mann who with Tim Spicer ran controversial Sandline International whose successor is Aegis Defence Services and is a British private military company with overseas offices in Afghanistan, Bahrain, Iraq, Kenya, Nepal and the US. Simon Mann was involved in the attempted coup in the Equatorial Guinea seeking to overthrow President Obiang..

The following are some notable private contracts from the past decade with estimates of their costs.

Firstly, Vinnell Corp for supplying and training the Saudi National Guard, the elite forces that protect the Saudi monarchy and maintain stability at an estimated cost of US\$831mio and for training a number of battalions of the Iraqi army at an estimated cost of US\$48mio.

Aegis Defence Services were contracted to provide security for the Programme Management Office monitoring the reconstruction effort in Iraq. The contract called for up to 75 two-man security teams trained in "mobile vehicle warfare" and "counter-sniping," and put Aegis in charge of coordinating all the private security contractors in Iraq at an estimated cost of US\$293mio.

Another case was DynCorp who were contracted to provide a security detail for Afghan President Hamid Karzai at an estimated cost of US\$52mio and contracted to create a new Iraqi police force at a cost of US\$50mio.

Erinys International were contracted to protect Iraq's oil pipeline, requiring 14,500 guards at an estimated cost of US\$39.2mio.

CACI Systems and Titan Corp were contracted to provide interrogation services in Iraq, including working at Abu Ghraib at an estimated cost of US\$19.9mio.

Executive Outcomes were asked to help defend Sierra Leone's capital, repelling an invading rebel army, and storming its stronghold. While under contract Executive Outcomes defeated two violent coup attempts by the rebel army, but a third internal coup did succeed which brought to power a head of state more sympathetic to Executive Outcomes at an estimated cost of US\$35mio.

Finally, Onix International provided a team of former New Zealand special-ops soldiers to rescue a businessman held hostage in East Timor for an estimated US\$20mio.

Real Estate Agents

"Ninety percent of all millionaires become so through owning real estate. More money has been made in real estate than in all industrial investments combined. The wise young man or wage earner of today invests his money in real estate."

Andrew Carnegie – Scottish businessman and philanthropist

Introduction

According to a FATF report titled, "Money Laundering & Terrorist Financing through the Real Estate Sector",³⁶ the use of real estate to launder money seems to afford criminal organisations a triple advantage, as it allows them to introduce illegal funds into the system, while earning additional profits and even obtaining tax advantages (such as rebates, subsidies, etc.). Non-financial professionals such as notaries, registrars, real estate agents etc., are sometimes used by suspected criminals on account of their central role in carrying out real estate transactions. Their professional roles often involve them in a range of tasks that place them in an ideal position to detect signs of money laundering or terrorist financing.

Definition/Description

FATF have identified a class of businesses they call, "Designated Non-Financial Professions and Businesses (DNFPBs)" being professions and businesses that are seen as being attractive to money launderers and these are: casinos, (when their customers engage in financial transactions above US\$/€3,000), lawyers, accountants and trust and company service providers, dealers in precious metals and stones (when their customers engage in cash transactions above US\$/€15,000) and real estate agents. A real estate agent or broker acts as a licensed intermediary between the seller and the buyer of real estate.

Buying property offers criminals an opportunity to integrate their laundered money by making an investment while also giving their criminal enterprise the appearance of financial stability. Buying a hotel, a restaurant or other similar investment offers further advantages, as it brings with it a business activity in which there is extensive use of cash and thus a steady, legitimate source of funds in which to come into and hide dirty money. Real estate is also purchased in order to facilitate further crimes such as trafficking in illegal immigrants in order to staff a recently purchased restaurant or factory or which may produce counterfeit or pirated goods.

With the real estate market being one of the largest markets in the world, prices can vary with some prices reaching very high levels and enticing those seeking luxury as well as status.

The most expensive house in the world is owned by Mukesh Ambani, an Indian billionaire and heir, alongside brother Anil, each to half of the Reliance Group of Companies, following the death of his father. Ambani has a net worth of US\$43bio and decided to build a new skyscraper in the centre of Mumbai, named Antilla for his wife and three children to live in, along with 600 staff. The 27 story (family home) skyscraper reputedly cost US\$2bio has a helipad, a health club, and a six-floor garage that can hold 168 cars. Each level has gardens.

Besides new builds, the most expensive purchase of a private residence was the Villa Leopolda on the Cote d'Azur, in France, for £390mio. The property has 20 acres of gardens, overlooks Cap Ferrat near Villefranche and was originally built as a summer retreat for King Leopold II of Belgium. Its new owner is believed to be one of the Russian oligarchs.

Whilst individual cities and properties have particular attractions, there are a collection of locations that continue and compete as the most expensive locations for real estate. According to UBS, Oslo, followed by Zurich and then Tokyo are the most expensive cities in the world to live while 70 places further down the list are occupied by Bucharest, Mumbai and Delhi. As far as pure real estate prices are concerned Monaco leads London and Hong Kong in the global rankings.

Real Estate Prices	
Country	Price per sq meter
1 Monaco	US\$53,000
2 London	US\$20,500
3 Hong Kong	US\$19,500
4 Paris	US\$18,000
5 Singapore	US\$17,000
6 Geneva	US\$15,500
7 Moscow	US\$14,000
8 Tokyo	US\$14,000
9 New York	US\$13,500
10 Mumbai	US\$13,000

Source: 257.com 2012 (numbers rounded up)

Beyond owned real estate, the most expensive rented accommodation is probably the Royal Penthouse Suite in the Hotel President Wilson in Geneva which costs US\$65,000 per night. This palatial suite, which occupies an entire floor of the hotel and measures 18,083 square feet, has 10 rooms and seven bathrooms. It was renovated in January 2009 to add a new private fitness area, according to a spokesperson.

Money Laundering/Terrorist Financing Risks

Beyond the legitimate high value real estate sector, there is another and as the FATF Report states, "Real estate transactions can be used to cloak illicit sources of funds or serve as legitimate front businesses, particularly if they are cash intensive. Properties may be bought and sold under false names or by shell corporations and can readily serve as collateral in further layering transactions." As a result, real estate agents are in a position to assist in money laundering or help in the fight against it. For that reason, the FATF included the business of buying and selling real estate as covered under Recommendation 5, 22 and 23 as referenced above.

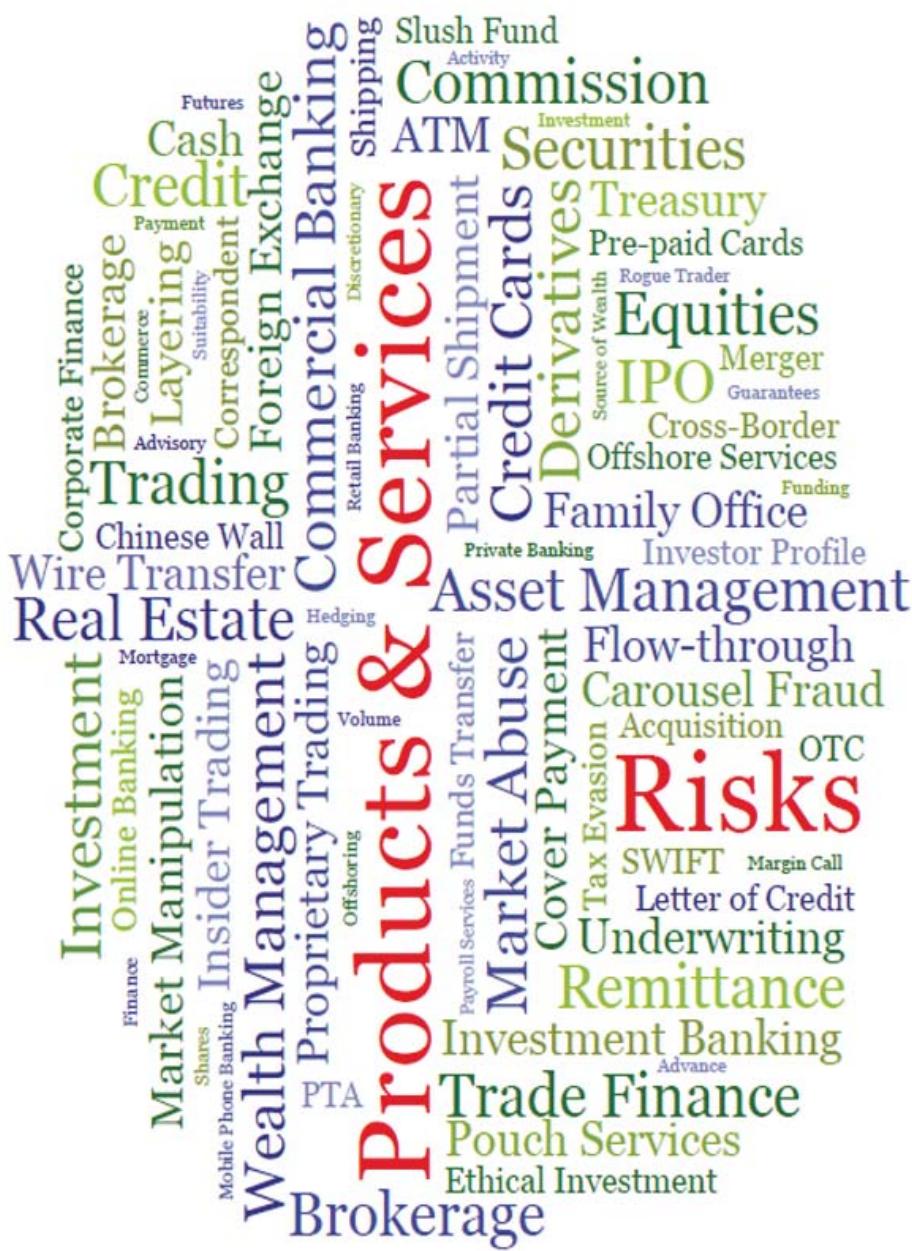
Real estate agents have been used by organised criminal gangs and drug traffickers to launder money by converting criminal proceeds into real estate assets. OFAC referenced the connection back in 1995 when US President Clinton issued an Executive Order to block assets and prohibit transactions with the Colombian drug cartels and launched their "Specially Designated Narcotics Traffickers" or SDNT programme. The SDNT list referred to "527 companies and 815 individuals involved in the ownership or management of the 21 Colombian drug cartel leaders' business empires. The businesses named as SDNTs ranged across industries and included drugstore chains, a supermarket chain, pharmaceutical laboratories, airlines, a medical clinic, hotels, restaurant service companies, radio stations, sports teams, communications companies, construction firms, real estate firms, investment and financial companies, consulting companies, offshore firms, horse breeding farms and other agricultural businesses, mining operations, maritime agencies, and a department store."³⁷

The Yakuza gang prominent in Hawaii, Yamaguchi-Gumi, is heavily into real estate there with significant holdings in several other states as well (California, Oregon and Washington). The Australian Federal Police also report that the Yakuza are laundering the proceeds of their crimes (committed elsewhere) through Australian real estate. Real estate was also connected to Human Traffickers in the 2011 FATF Report "Money Laundering Risks Arising from Trafficking in Human

Beings and Smuggling of Migrants", when the use of cash to invest in real estate was cited. Another risk that should not be overlooked when dealing with real estate agents is indirect sanctions risks.

The FATF report on "RBA Guidance for Real Estate Agents"³⁷ supports the development of a common understanding of what the risk based approach involves and outlines the high-level principles involved in applying the approach as well as best practices in the design and implementation of an effective risk based approach. In addition, the FATF report titled, "Money Laundering & Terrorist Financing through the Real Estate Sector" lists red flag indicators that relate to the real estate agent's customer and components of the transaction to which the financial institution may not be involved.

A few broader red flag indicators include: (i) Transfer of real estate between parties in a time period that is unusually short with no apparent legitimate reason; (ii) Money coming in from abroad related to real estate purchase. Hard to assess property worth especially in other countries where it varies from region to region; (iii) Non-disclosure of underlying client. Real estate agent setting up account to purchase the property, not disclosing actual buyer, money coming from buyer not disclosed; or (iv) Unusually high fees/commissions for real estate transaction that would not ordinarily warrant such a premium.



Sub-section 3. Products & Services (incl Channels) Risks

- A Brief History of Banking, 179
- Asset Management, 181
- Brokerage / Securities, 183
- Commercial Banking, 186
- Correspondent Banking, 191
- Credit & Other Cards, 198
- Investment Banking, 201
- Retail Banking, 205
- Wealth Management/Private Banking, 209

A Brief History of Banking

Banks have been around since the first currencies were minted, perhaps even before that, in some form or another. Currency, particularly the use of coins, grew out of taxation by rulers and as empires expanded, coins of varying sizes and metals that could be exchanged easily served as a way to pay for foreign goods and services. These coins, however, needed to be kept in a safe place. Ancient homes did not have the benefit of a steel safe, therefore, most wealthy people held accounts at their temples, where priests or temple workers were trusted as both devout and honest, but over time, records from Greece, Rome, Egypt and Ancient Babylon suggest temples also loaned deposited money out, in addition to keeping it safe. The fact that most temples were also the financial centres of their cities, is the major reason that they were ransacked during wars.

The Romans took banking out of the temples and formalised it within distinct buildings and so began the distinct trade where moneylenders profited from taking in and lending money. Julius Caesar, in one of the edicts changing Roman law after his takeover, gives the first example of a major shift in power between lender and landowner allowing moneylenders to confiscate land in lieu of default in loan repayments.

After the fall of Rome, banking was largely abandoned in Western Europe and did not revive until the time of the crusades, in the form of papal and other powerful bankers, that emerged in the Holy Roman Empire. Outside the papal institutions, banking became subject to additional restrictions, as the charging of interest was seen as immoral, equally so on the face of it under Islam and Judaism. Whilst some interpret for example the Jewish Torah as forbidding the charging of interest only by Jews to other Jews and not to non-Jews, or Gentiles, the involvement of Jews in the money lending business is likely much more to do with the fact that by the time of the Middle ages, Jews were ostracised from most professions by local rulers, the Church and the guilds and so were pushed into marginal occupations considered socially inferior, such as tax, rent collecting and money lending.

As commerce expanded, innovation played its part and bills of exchange were created as a means to avoid the carrying of coins and large chests of treasure around. Money changers at merchants fairs issued documents redeemable at other fairs, in exchange for hard currency. These documents could be cashed at another fair

in a different country or at a future fair in the same location. If redeemable at a future date, they would often be discounted by an amount comparable to a rate of interest, or for an equivalent fee, much as today's Hawaladers and the like operate.

With finance available for trade, both local and international, both commerce and those that controlled finance largely prospered. The term moneylenders had already morphed and now those involved became known as bankers, through the term "bank," - banco, banque, bank each meaning, "bench" or "counter" where the moneylender sat usually with some of his money in plain sight in fairs to town squares. When a banker was no longer solvent the bench would be smashed or ruptured and the banker declared, "bankrupt". Amongst bankers, there developed a hierarchical order. At the top were the bankers who did business with heads of state, next were the city exchanges, and at the bottom were the pawn shops or "Lombards". The most advanced bankers in the middle ages were those from Italy seen as the pioneers of modern banking, for example the "Medici" Bankers in Florence, who not only influenced other Italian bankers but also many more in Germany, France, The Netherlands, Switzerland, England, Spain and elsewhere. Whilst some of those at the top of the banking hierarchy did well from dealing with sovereigns, others did not. Some of the royal powers began to take loans to make up for hard times at the royal treasury, often on the king's terms. For example in 1557, Phillip II of Spain borrowed so much to fight war after war, that he caused the world's first national bankruptcy, as well as the second, third and fourth, in rapid succession. This occurred because 40% of the country's gross national product (GNP) was going toward servicing the debt. Spain never recovered and was quickly surpassed in the late 17th century, by its once fierce rivals whose largest centres for commerce also housed the main centres for banking, being the ports of Amsterdam, London, and Hamburg.

Banking at this time, largely consisted of private banking for the wealthy and commercial banking for trade. As far as private banking and then personal banking, innovation in Amsterdam in the 16th Century led to the introduction of charges for customers for depositing their wealth for safekeeping, a practice that soon spread to the UK. Competition led these bankers to offer other services, including paying out money to any person bearing a written order from a depositor to do so. Britain became a major innovator in the banking world. According to the Payments Council, which represents UK banks, half of the 10 oldest continuously operating banks in the world are in the UK. British

banks invented many of the current account features we now take for granted. Pre-printed cheques appeared in the 18th century, together with a clearing system that involved bank clerks meeting at the Five Bells tavern in Lombard Street, to exchange all their cheques in one place and settle the balances in cash.

In 1778, the Royal Bank of Scotland invented the overdraft. The bank allowed William Hog, a merchant, to take £1,000 (the equivalent of £63,664 today) more out of his account than he had in it. In those times, bank accounts were a luxury for the rich, something that didn't change for more than 200 years. Banking expanded beyond the wealthy to cover also the middle classes and specialised with merchant banks, who used national and international connections, political and financial power and the knowledge and practices of markets to prosper, none more than JP Morgan and Company. JP Morgan and Company emerged at the head of the merchant banks during the late 1800s, exerting great influence over American industry, creating for example, US Steel and AT&T and creating great oligopolies across American Industry. JP Morgan also almost single-handedly halted the Panic of 1907 by quickly persuading all the major players on Wall Street to work towards stability and back a recovery, just as a central bank would do today.

Ironically, despite this act of courage and its successful outcome, JP Morgan and those other so called "robber barons," alongside Carnegie and Rockefeller, as beneficiaries of consolidation were so disliked that the US Government established its own Central Bank in 1913, the Federal Reserve, and started to break up first the monopolies and oligopolies and then after the Great Crash of 1929 even broke up JP Morgan & Co.

With the increasing size of newly formed industrial companies, the amounts needed for growth, could no longer be provided by any one bank, so merchant banks managed IPOs and bond offerings, raising money directly from the public in order to generate sufficient funds. With such offerings, the public in the US, Europe and elsewhere, began to take a greater interest in investments, banks became commonplace and most citizens would open bank accounts for retail services, including taking credit and debit cards. Commerce would still require funding for trade, international payments would increase as would domestic payments, savings and investment products would be taken up by individual customers as well as pension funds and insurance companies, requiring asset management services and merchant banking would transition into investment banking as we see it today.

Banking eventually became available to ordinary households, with many in the developed and developing world gaining access to bank accounts, with it becoming increasingly difficult to function without one. Charge cards were invented in the US in the 1950s quickly followed by credit cards; (for more details see Credit and Other Cards below) and the ATM (see for more details Retail Banking below) deployed by Barclays Bank in London in 1967. Traditionally, bank customers managed their money using a passbook that they took into their branch every time they wanted to pay in money or take it out. However, most bank customers do not need to go into a branch on a regular basis as they can do most of their banking either online, on the telephone or by using a cash machine. As well as in-branch queuing, personal attention from the bank manager has largely become a thing of the past. Most queries on a bank account are now managed by call centres or branch staff who have little or no information on individual clients other than that held on a computer.

Banks have come a long way from the temples of the ancient world, but their basic business practices have not changed. Banks take in peoples money, keep it safe, but at the same time invest it and make those monies grow in value, by numerous means, including providing services such as credit to people who need it, but demand interest as a fee for this service, or providing advice or other services, such as converting or exchanging money or transferring monies.

Although history shows the continued development and innovation within banking, much remains inherently the same. Even if the future takes banks completely off the high street and onto the internet, or more likely via the mobile phone, Banks will remain at the heart of most people's financial experiences for a long time to come. In the sections that follow, there is a brief summary for each of the main types of banking businesses that proliferate today, together with an explanation of the main inherent money laundering and terrorist financing risks that they face. The areas of banking covered are: asset management; brokerage/securities; commercial banking; correspondent banking; credit and other cards; investment banking; retail banking; and wealth management/private banking. The Worlds largest banks by assets can be found in Part 1 Section 2 Sub-Section 2 Customer Risks; Banks and Other Financial Institutions. Whilst some Banks specialise in one of these areas, others more than one, still others considered so called universal banks cover all areas of banking. Few banks are the same, though and each should ideally consider the risks for themselves.

Asset Management

"Don't put all your eggs in one basket"

Well known proverb

Introduction

There is nothing certain in life perhaps with the exception of death and taxes, and the same goes for investments. Whilst investments generally may grow in a bull market, (especially when leveraged), lose value in a bear market (especially when leveraged), increase in value the longer they are invested (lose value the more transactions are undertaken; often due to transaction fees); reduce downside risk by asset class by applying principles of diversification, reduce sovereign and country risk by applying the principles of global diversification; benefit by individual expert stock picking (and fortune) or are harmed by cack-handed opportunists (and bad luck), what remains is a huge amount of investment capital, the oxygen of capitalism running through the veins of the global economy, giving life to some, nourishing many, reaping the benefits from those that flourish and extracting the last breath from those that are no longer considered sustainable.

Despite these investment let alone home truths, the search for a simple positive return and more than this, relative positive return (known as alpha) or predictable risk adjusted returns (known as beta) remains the holy grail for consistent professional asset managers.

Definition/Description

Asset managers, aggregate funds into a significant amount and invest these funds on the basis of representations and promises, looking to meet or beat these representations and promises. Asset managers can be both discretionary and advisory, they can track an index, or invest in a sector, country, region, principle or idea. Where once the industry told the investor what to commit funds to, today the industry caters for individual tastes and styles and competes within each and for individual and professional investors. Leading asset management companies will usually offer a wide range of investment products and services. Typical offerings include i) Equities: core global, regional, country and emerging markets; opportunity, high alpha; small cap, sector, thematic, sustainable; growth style, global US, emerging markets; long/ short, unconstrained, market neutral rules based, high dividend; indexed ETFs; multi-strategy; ii) Fixed Income: global; country and regional; money market; short duration; core and core plus; sector specific; emerging markets; high yield; indexed, ETFs; unconstrained; customised solutions; iii) Global

Investment Solutions: global; country and regional; asset allocation; currency management; return and risk targeted; structured portfolios; risk management; advisory services; multi manager. iv) Fund services: fund/product set-up; NAV calculation; middle office services; reporting; investor services; private labelling; international distribution support; ancillary services for fund of hedge funds. v) Alternative and Quantitative Investments: single manager hedge funds; multi- manager hedge funds; advisory services; quantitative; active Commodities multi-manager; vi) Global Real Estate: vii) Infrastructure and Private Equity.

Total assets under management managers totalled US\$35 trillion at end-June 2013 according to EFAMA, Investment Fund Industry Fact Sheet.

Top 10 / 500 World's Largest Asset Managers (US\$ trillion)			
No	Manager	Home	Assets
1	Blackrock	US	3.5
2	Allianz	Ger	2.1
3	State Street	US	1.9
4	Vanguard	US	1.8
5	Fidelity	US	1.7
6	JPMorgan Chase	US	1.3
7	BNY Mellon	US	1.3
8	BNP Paribas	Fr	1.2
9	Capital Group	US	1.1
10	UBS	CH	0.95

Source: Towers Watson 2012 - 2011 figures²

Money Laundering/Terrorist Financing Risks

Asset management is considered generally lower to moderate risk, particularly in typical situations, for example, for customers, including from domestic pension funds including from publicly owned companies and listed companies; well respected banks such as private banks investing both mass retail and private banking customer's funds; insurance companies investing premiums; and direct individual investors, both high net worth, and mass retail making up and aggregating into collective investment funds. In most cases, all money and other assets within the portfolio are held under the control of a regulated custodian, with money paid to or from the customer through their own bank account. Asset management is not a mechanism for the movement of assets from one person to another, although some third party payments may be made, hence for all these reasons.

Asset management is considered generally to present **low to moderate** inherent AML risks for money laundering purposes. Low risk doesn't mean risk free and asset management is potentially vulnerable to and/or could be abused in a number of ways. Here are the top inherent ML related risks facing an asset manager:

Top ML Risks for an Asset Manager	
1	Sensitive customers
2	Customers with material sensitive country risk exposures
3	Politically Exposed Persons
4	Charities or other not for profit organisations
5	Sanctioned or other problematic customers
6	Fraud
7	Employee/market abuse

Source: Author

1. Sensitive Customers

Customers that could be involved in activity that is itself considered sensitive or controversial, for example, agreeing to manage funds from businesses such as; arms dealer companies or private military firms; businesses that make and/or distribute war materials, in particular controversial weapons (nuclear, chemical or biological or cluster munitions and anti-personnel mines) or dual use goods, businesses involved in mining and minerals, particularly if involved in so called, mountain top removal, forestry or logging businesses, particularly if involved in palm oil extraction or leading to deforestation; businesses with poor human rights records or a record of environmental damage; businesses involved in waste management, infrastructure and real estate funds.

2. Customers with Material Sensitive Country Risk Exposures

Customers, in particular sensitive customers, that are based in or have material exposures to countries that have been identified as posing increased risks, for example countries the subject of sanctions and/or embargoes, with major corruption problems, organised crime and terror finance/WMD proliferation concerns. This also for customers owned or controlled by or dealing with sovereign governments and publicly owned entities from such countries, including sovereign wealth funds and municipalities, also funding for large infrastructure projects. For more details see Part 1, Section 1, Bribery & Corruption; Terrorism Finance & WMD Proliferation Finance and Part 1, Section 3, Sanctions & Embargoes.

3. Politically Exposed Persons

Customers whose funds could be for the benefit of, ultimately controlled by or directed by Politically Exposed Person's where such persons could be considered corrupt or similarly involved in criminal activity; that is, the personal pension fund of a kleptocrat. For more details see Part 1, Section 1, Bribery and Corruption and Part 1, Section 2; Politically Exposed Persons.

4. Charities or other Not for Profit Organisations

Charities or other Not for Profit Organisations, which could be either effectively or insufficiently unsupervised that raise, store, move and/or use money for charitable and other humanitarian causes that are either subject to an applicable sanctions listing, or are otherwise identified by credible sources as connected and/or involved in terrorism finance. Organisations providing humanitarian or other similar relief have been used and abused in particular as fronts for Islamic terrorism financing. For more details see Part 1, Section 2, Charities and Not For Profit Organisations:

5. Sanctioned or Otherwise Problematic Customers

Customers that are either subject to an applicable sanctions listing, or are otherwise identified by credible sources as may be connected and/or involved in criminal activity, including corruption, terrorism finance, WMD proliferation etc. Asset managers must be wary in particular to screen customers, for example, against known terrorists and major criminals against lists of persons made available prior to conducting business and against payment flows if to other parties. Also relevant are concerns over securities affected by sanctions. For more details see Part 1, Section 3, Sanctions & Embargoes.

6. Fraud

Investment opportunities that may look too good to be true or have increased fraud risks may not be true. For more details see Part 1, Section 1, Fraud.

7. Employee/Market Abuse

Asset Managers especially large ones, with large orders may find that some of their money laundering risks are actually quite close to home. These include insider dealing for star asset managers, front and parallel trading for others and/or market timing/late trading and other abuses of the market. For more details see Part 1, Section 1, Insider Trading and Market Manipulation.

Brokerage / Securities

"And there is no such thing as a no sale call. A sale is made on every call you make. Either you sell the client some stock or he sells you a reason he can't. Either way a sale is made, the only question is who is gonna close? You or him? Now be relentless, that's it, I'm done."

Jim Young in the movie "Boiler Room"

Introduction

The brokerage/securities industry is one of the core industries, along with banking and insurance, through which persons and entities can access the financial system. The industry is known for its speed in executing transactions, its global reach, and its adaptability; all features that make it attractive to money launderers and terrorist financiers. Additionally, the securities industry is in a unique position to be used to both launder illicit funds obtained outside the sector, and to generate illicit funds within the industry itself through fraudulent activities such as insider trading, market manipulation and (securities) fraud, all "Designated categories of offences" in the FATF 40 Recommendations.

Definition/Description

A brokerage firm is a financial institution that facilitates the buying and selling of financial securities between a buyer and seller; the broker gets a fee or commission when the deal is executed. The term "Security" or "Securities" is not defined in the Glossary of the FATF 40 Recommendations; probably because countries differ in the types of products that they define as Securities. Investopedia defines security as "a financial instrument that represents: an ownership position in a publicly-traded corporation (stock), a creditor relationship with governmental body or a corporation (bond), or rights to ownership as represented by an option. A security is a fungible, negotiable financial instrument that represents some type of financial value."³³ Depending on the jurisdiction, trading in securities is often not limited to securities broker-dealers, but can also involve the banking and insurance industries.

In the US, brokerages are sometimes called "wirehouses" but can also be part of banks, private banks, investment advisers and can operate as discount or online brokers. With increasing consolidation of the main players in the US brokerage business into banks some call these "bankerage". Some unregulated and illicit operations have tried to defraud investors through the operation of so-called "Boiler Rooms". For details see Part 1, Section 1, Market Manipulation.

Top US Brokerages			
No	Name	Advisers	Assets trillion
1	BofA Merrill Lynch	15,000	US\$1.58
2	Morgan Stanley	18,000	US\$1.67
3	Wells Fargo Advisers	15,000	US\$1.2
4	UBS	6,800	US\$0.806

Source: Author

Whilst many investors with significant sums of money will choose to invest via one of the leading brokerages and/or via a typical broker that offers face to face and/or one to one communication, others who value cost and market access over communication and advice may prefer online brokers, and are known as self directed investors. These online brokers can be found all over the world, with the largest concentration being in the US and with services such as a stock trading service you can buy and sell stocks, options, mutual funds, exchange-traded funds and various fixed-income securities including bonds and CDs. Many online stock market investing services offer investment options such as retirement and investment funds for education or retirement and online stock market trading services also offer useful tools such as alerts, watch lists, third-party analyst reports, option chains, investment calculators and virtual trading.

According to TopTenREVIEWS the following, are the top 10 online brokers in the US, evaluated using a number of commercial factors (<http://online-stock-trading-review.toptenreviews.com/>).

Top 10 US Online Brokers	
1	OptionsXpress
2	OptionsHouse
3	TradeKing
4	Scottrade
5	Fidelity
6	E*Trade Financial
7	Charles Schwab
8	TD Ameritrade
9	ShareBuilder
10	Firstrade

Source: toptenreviews 2013

Money Laundering/Terrorist Financing Risks

Money laundering risks with securities or brokerage activity takes place since broker-dealers generally do not accept cash, in the layering and integration stages. According to the 2009 FATF Report "Money Laundering and Terrorist Financing in the Securities Sector"³⁴ typical securities related laundering schemes often involve a series of transactions that do not match the investor's profile and do not appear designed to provide a return on investment. Since a key to laundering illicit proceeds is the ability to change them from their original form and ownership by layering transactions, transferable securities should not be overlooked for this process. Now that broker/dealers and other financial institutions that handle securities have more robust AML transaction monitoring programmes, the laundering techniques have become more complex and involve trading and transferring of securities, and the commissions or fees paid are just considered the cost of laundering the illicit funds. In fact, in some cases such as pump and dump schemes or insider trading, the proceeds from the trading itself are the illicit funds that need to be laundered.

Brokerages can generally be considered as presenting **moderate to high** inherent AML risks, however brokerage is still potentially vulnerable to and/or could be abused in a number of ways.

Here are the top inherent AML related risks facing a securities broker.

Top ML Risks in Brokerage	
1	Customers with cash businesses
2	Customers with sensitive businesses
3	Customers with material sensitive country risk exposures
4	Complex or complicated non transparent customers
5	Politically Exposed Persons
6	Sanctioned or other problematic customers
7	Fraud, including market abuse
8	Tax evasion
9	Employees
10	Customers with physical or bearer securities

Source: Author

1. Customers with Cash Businesses

Customers that have businesses that deal in cash in large amounts, high value and/or with a large number

of transactions are highly vulnerable to being used by money launderers as a vehicle to convert and launder the proceeds of crime. There are few high value and/or retail businesses that could not be used though a few are considered particularly vulnerable and these include; high value goods dealers, for example; real estate agents; art dealers including (auctioneers); precious metals and stones dealers (including jewellers); car, plane and yacht dealers; watch dealers, equine or other high bred animals; and cash intensive businesses including; retail outlets such as garages, restaurants, ice cream parlours, clubs (including strip bars) and bars, golf clubs, bowling alleys, private ATM companies, sauna and massage parlours and of course laundromats. Customers owning such businesses may further wish to launder or to invest criminal proceeds. There are some businesses that could fall into both categories and these include; money service businesses, both regulated and unregulated; jewellers; auctioneers and casinos. For more details on some of these businesses see Part 2, Section 2, Sub-section 2, Cash-Intensive Businesses, High Value Goods Dealers, Real Estate Agents and Precious Metals & Stones Dealers.

2. Customers with Sensitive Businesses

Customers involved in arms dealing or in private military firms; customers involved in making and/or distributing war materials or dual use goods may present additional risks. Customers involved in mining and minerals, particularly if involved in so called, mountain top removal, forestry or logging businesses, particularly if involved in palm oil extraction leading to deforestation; businesses with poor human rights records or a record of environmental damage; Customers involved in waste management and scrap metal dealers and businesses that have been identified as posing increased corruption risks themselves, particularly when combined with increased country risks, including with intermediaries as set out in 3. below. For more details see Part 1, Section 2, Sub-section 1, Money Laundering Risks.

3. Customers with Material Sensitive Country Risk Exposures

Customers, in particular sensitive customers, that are based in or have material exposures to countries that have been identified as posing increased risks, for example countries the subject of sanctions and/or embargoes, with major corruption problems, organised crime and terror finance/WMD proliferation concerns. For more details see Part 1, Section 1, Bribery & Corruption; Terrorism Finance & WMD Proliferation Finance and Part 1, Section 3, Sanctions & Embargoes.

4. Complex or Complicated Non-Transparent Customers

Customers, who are unduly or excessively complex, where identification and/or due diligence is difficult to establish or carry out satisfactorily, for example, customers operating through personal investment companies or numerous layers of holding vehicles which appear designed to hide the ultimate beneficial owner. For more details see Gatekeepers in Part 1, Section 2, Sub-section 2.

5. Politically Exposed Persons

Customers who are Politically Exposed Persons including Sovereign Wealth Funds. For more details see Part 1, Section 1, Bribery and Corruption and Part 1, Section 2, Sub-section 2, Politically Exposed Persons.

6. Sanctioned or Otherwise Problematic Customers

Customers that are either subject to an applicable sanctions listing, or are otherwise identified by credible sources as may be connected and/or involved in criminal activity, including corruption, terrorism finance, WMD proliferation etc. Brokerages must be wary in particular to screen customers, for example against known terrorists and major criminals against lists of persons made available prior to opening of accounts and against payment flows if to other parties. For more details see Part 1, Section 3, Sanctions & Embargoes.

7. Fraud including Market Abuse

Customers that indicate they could be operating a Boiler Room operation and/or other customers dealing in a manner raising concerns of market abuse, including insider dealing, misuse of information and market manipulation. Customers that are themselves insiders may present additional risks in some circumstances. For more details see Part 1, Sections 1, Fraud; Insider Dealing and Market Manipulation.

8. Tax Evasion

Customers that are non resident for tax purposes, may use a brokerage account to invest sums undeclared for tax purposes and use the services of the brokerage to hide these investments. A brokerage should never assist a customer in cheating its taxes, and if it becomes aware or suspects that a customer is cheating on its taxes, then it should, where tax crimes are predicate offences to money laundering, file appropriate suspicious activity reports. For more details see Part 1, Section 1, Fraud, Tax Fraud & Cybercrime.

9. Employees

Brokerages may find that some of their money laundering risks are actually quite close to home. These include insider dealing by financial advisers, through

relationships with customers who may be themselves "insiders", or as a result of working in a universal bank with an investment bank and getting unauthorised access to information or being tipped off or through other outside contacts; for misuse or interaction through front and/or parallel trading in connection with large customer orders. Also a financial adviser may exceed his authority with respect to customer activity and/or divert customer assets for his own benefit whether to make personal gain or to cover earlier undisclosed losses. For more details see Part 1, Sections 1, Fraud and Inside Information and Market Manipulation.

10. Customers with Physical or Bearer Securities

Although many jurisdictions have dematerialised securities, physical and bearer securities are still available in some jurisdictions. Bearer securities consist of both physical equity and debt securities that, unlike registered securities, do not necessarily require that the owner be registered with an issuer or a transfer agent. The transfer of bearer securities can be as simple as handing the security over to a new owner. It is important to note that the transfer of ownership can, in some jurisdictions, be almost as easily accomplished through electronic means that inhibit tracking any change of ownership. In addition, some bearer bonds are almost equivalent to cash because they can be easily redeemed at financial institutions. Low priced securities, also known as "Penny Stocks", refer to low-value equity interests in companies that are publicly traded or are about to become so. The issuers of these shares generally have legitimate business operations and revenue streams. However, some of these publicly traded entities are really shell companies that may be used for a reverse merger. In any event, shares in these issuers will often be represented with physical securities that can be deposited with a securities intermediary. These shares are not likely to be traded on traditional exchanges, but rather in over-the-counter ("OTC") markets or on bulletin boards. Penny stocks typically have very low trading volume but, unlike bearer securities, ownership of these shares will often be registered with the issuer and/or a transfer agent. These securities can be acquired by investing illicit assets into a company that is about to become public. Once the company goes public, the money launderer can sell his or her stake, thereby giving funds the appearance of having been derived from a legitimate securities transaction. In addition, Penny Stocks are often used to generate illicit assets through market manipulation, insider trading, and fraud. For more details see Part 1, Section 1, Fraud; Insider Dealing and Market Manipulation.

Commercial Banking

"Adventure is the life of commerce but caution, I had almost said timidity, is the life of banking"

Walter Bagehot, 19th century British economist & journalist

Introduction

Commercial and corporate banks have existed for as long as businesses have had the need to borrow funds. Without access to credit, many businesses either stall or find growth elusive. This is not only bad for the businesses themselves but for the broader economy and ultimately individual living standards. As banks recover from the global financial crisis of 2008, the availability of credit will increase and once more be a catalyst for economic growth. The importance of banking and in particular commercial banking should not be underestimated, both in its crucial role in developing and achieving strong, sustained and balanced growth through the ages up until now, despite the crises and its undoubtedly role in driving economic growth in the future.

Whilst financial systems and the availability of credit, particularly to support business and commerce, have long been recognised as useful, their true importance and the fact that they play a key role in economic development and growth, only received academic validation and widespread recognition approximately 50 years ago when Gurley, Shaw and McKinnon⁶ published their studies, since accepted by the IMF and World Bank.

According to their analysis, a strong financial system and the availability of credit to finance business expansion and innovation made possible the Industrial Revolutions in the West and in particular in the US where the commercialisation of technological innovation in 19th century America, beginning with the adaptation of railway engines and moving rapidly to completely new technologies, such as the telegraph and telephone as well as the creation of a truly national market were but a few examples of the importance of commercial banks.

Whilst commercial banks offer more than credit to businesses, including international trade finance, and for example, traditional retail banking and payment services, there are money laundering risks that present themselves and should be addressed.

Definition/Description

Commercial banks offer banking, credit and payment services to businesses, usually alongside similar retail

banking services to individual customers. Commercial banking customers are usually both small and medium sized enterprises (SMEs) and larger businesses, for example, major companies, or conglomerates and multinationals. Some of the products and services Commercial Banks offer include: credit and financing services (that is, asset-based lending, commercial term lending, equipment financing, capital raising and trade financing), treasury management (that is, collecting and control of payments and deposits and liquidity management) and acquisition financing. For the larger customers, commercial banks can issue large secured and unsecured loans, offer fund transfer services, cash management and treasury services and may offer similar products and services or refer customers to their investment banking division to cover, for example, needs for the issuance of securities, arranging and underwriting services for debt issuance, initial public offerings and advice on corporate restructuring and on mergers and acquisitions.

Trade Finance

One of the oldest and most popular products offered by Commercial Banks but cited as vulnerable to money laundering is Trade Finance. Trading, especially internationally, has historically required two key elements, trust and finance. Trust is especially important as the buyer and seller may have little knowledge of each other and finance is important because the goods may leave the exporter and not be received by the importer until delivery weeks later. Banks have sought to interpose themselves into international trade providing not only finance but the requisite trust to guarantee that provided the goods are shipped, documented and delivered, payment will be made. In this way banks have helped international trade flourish with about US\$18 trillion of goods exported in 2011, (ICC Banking Commission, 2013 Global Risks Trade Finance). Whilst most trade is now financed by the importers and exporters themselves on their "own account" that is directly without credit finance, in the normal way that firms have become accustomed to do so in their domestic markets, still, according to the International Chamber of Commerce (ICC), around 20% remain financed by Banks. A significant portion of this financing involves a letter of credit, which provides greater security to the exporter and is particularly popular with small firms and in developing countries. Regardless of the type of financing exporters can also buy export insurance to reduce risk, with about 11% of world trade insured in 2009. According to Swift figures in 2011, 75% of total trade traffic flows, through the system was for documentary credits, with the two largest intra region trade areas being APAC and the Middle East. APAC as a region generated the most in both

import 65% and export 72% with the Eurozone second in both cases with 10% and 11% respectively.

The US\$ was the currency used in more than 80% of Swift Trade Messages, followed by the € at 12% and JPY at 4%. The average value of a letter of credit in 2011 was US\$603,000 (ICC Global Survey 2012, Rethinking Trade and Finance). There are a number of important products offered in connection with the financing of trade, used by exporters and importers, that are not comfortable taking the risk of cash or product in advance, or part advance that is, own account or on consignment, where the goods are shipped but not sold and legal title does not pass until actual payment, whether in part or in full. Although most trade finance is short term and self liquidating in nature, medium term loans (1-5 years) and long term loans (over 5 years) may be used to finance the export of capital goods such as machinery and equipment. The most common products include: Letters of Credit: the purchaser (importer) wishing to reduce risk may require the seller to document the goods that have been shipped, taking a letter of credit from his bank and providing this to the exporter (or the exporter's bank) providing for payment upon presentation of certain documents, such as a bill of lading. The exporter's bank may make a loan (by advancing funds) to the exporter on the basis of the letter of credit. In other words, if the buyer defaults on the payment, it is the responsibility of the buyer's bank to make the payment. This undertaking can be given either in writing or through authorised electronic medium. Other forms of trade finance can include documentary collection, standby letters of credit and/or guarantees, trade credit insurance, export factoring, and forfeiting. In many countries, trade finance in key or strategic industries, is often supported by quasi-government entities known as export credit agencies that work with commercial banks and other financial institutions.

The international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organisations with the opportunity to launder the proceeds of crime and move funds to terrorist organisations with a relatively low risk of detection. Whilst the abuse of the trade system is much more likely the abuse of trade finance products remains possible. The involvement of multiple parties on both sides of any international trade transaction and because trade finance can be more document-based than other banking activities, it can be susceptible to documentary fraud, which can be linked to money laundering, terrorist financing, or the circumvention of sanctions or other restrictions (such as export prohibitions, licensing requirements, or controls). For letters of credit and bills

of collection, two of the main products within trade finance, the commercial bank, will of course conduct due diligence on its own customer and on the bank with which it is dealing, but not usually on the customer's customer or the other bank's customer (that is, the same other party or the beneficiary) as this should be done by the Customer and/or the other Bank, though there may be occasions where this may be necessary, for example, if such a party or transactions posed increased risks. Banks are heavily dependent upon the information provided in the documentation submitted by the customer. The degree of scrutiny will often vary depending upon the product offered, the role in the transaction, and the geographies and traded goods involved. A review of the countries involved in the transaction, the type of goods involved, whether there is a third party or intermediary involved and if there are any anomalies in the documentation that suggest suspicious or illegal activity, may indicate increased risks. In particular transactions involving countries subject to sanctions and embargoes or involving higher-risk goods (for example, trade in weapons or nuclear equipment), will obviously require increased attention. As always with any transaction, screening customers against applicable lists should be commonplace. Beyond these controls it should be understood that whilst commercial banks oil the wheels of commerce through trade finance they are rarely in a position or have the capacity to become experts in what is and what is not dual use goods for example and/or understand fully the underlying economics of all trade transactions, to positively prove or demonstrate evidence to verify the efficacy of the goods involved, nor to verify the actual goods traded are those that are the subject of the trade finance transaction. Government agencies including law enforcement, customs authorities, and intelligence agencies are best placed to prevent and detect trade laundering. Additional scrutiny to be considered in exceptional cases include additional KYC or information such as frequency and number of transactions, volumes of the goods (for example, in relation to the client's production capacity), amounts involved (in absolute terms as well as in relation to the goods), diversity of counterparties and frequent irregularities in the settlement of a trade finance transaction.

While banks should be alert to risks presented by organised crime, terror finance and WMD proliferators including sanctions busters, they also need to consider and be aware that goods may be over, or under-valued in an effort to move funds or value across national borders, including to avoid customs or capital control regulations. For example, an importer may pay a large sum of money from the proceeds of an illegal activity for goods that are essentially worthless and are

subsequently discarded. Alternatively, trade documents, such as invoices, may be fraudulently altered to hide the scheme. Variations on this theme include inaccurate or double invoicing, partial shipment of goods (short shipping) and the use of fictitious goods. Illegal proceeds transferred in such transactions thereby appear sanitised and enter the realm of legitimate commerce. Moreover, many suspect trade finance transactions also involve collusion between buyers and sellers. For more details on so called trade based money laundering see Part 1 Section 1 Fraud including tax fraud and cybercrime. Financial crime risks in trade finance was investigated by UK FCA in its 2013 thematic review entitled "Banks' control of financial crime risks in trade finance" which found that whilst banks had developed effective controls to ensure they were not dealing with sanctioned entities and individuals, policies and procedures and controls to counter money laundering risk were generally weak and most bank's had inadequate systems and controls over dual use goods.

The main findings were that there was an inconsistent approach to risk assessment and only a few banks had conducted a specific trade finance money laundering risk assessment. About half the banks had no clear policy or procedures dealing with trade based money laundering risks, few banks produced useful management information on financial crime risks in trade finance businesses, smaller banks had not produced tailored training, and many AML Compliance staff were inadequately aware of money laundering risks for trade finance. Naturally the sophistication of the money laundering prevention programme adopted by a bank should be commensurate with the size and complexity of the bank's trade finance portfolio and its role in the trade finance process. The Money Laundering Prevention Programme should consider and give greater scrutiny to: items shipped that are inconsistent with the nature of the customer's business (for example, a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals); customers conducting business in higher-risk jurisdictions; customers shipping items through higher-risk jurisdictions, including transit through higher-risk jurisdictions; customers involved in potentially higher-risk activities, including activities that may be subject to export/import restrictions (for example, equipment for military or police organisations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore and crude oil); obvious over, or under-pricing of goods and services; obvious misrepresentation of quantity or type of goods imported or exported; transaction

structures that appear unnecessarily complex and designed to obscure the true nature of the transaction; customer payments of proceeds to unrelated third parties; shipment locations or description of goods not consistent with letter of credit; significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Absent indicative increased risk factors and unless customer behavior or transaction documentation appears unusual, the bank should not be expected to spend undue time or effort reviewing all information.

Top 10 Goods traded internationally (US\$ trillion)		
1	Mineral fuels, oils, distillation products etc	2.1
2	Electrical, electronic equipment	1.8
3	Machinery, nuclear reactors, boilers	1.76
4	Vehicles other than railway	1.1
5	Plastics and articles thereof	0.47
6	Optical, photo, technical, medical apparatus etc.	0.46
7	Pharmaceutical products	0.44
8	Iron and steel	0.38
9	Organic chemicals	0.377
10	Pearls, precious stones, metals, coins	0.35

Source: <http://in.finance.yahoo.com/photos/the-world-s-top-10-traded-goods-1366353488-slide-show2013>

Money Laundering/Terrorist Financing Risks

Commercial banking can generally be considered as presenting **moderate to high** inherent AML risks.

Top ML Risks in Commercial Banking		
1	Customers with cash businesses	
2	Customers with sensitive businesses	
3	Customers with material sensitive country risk exposures	
4	Politically Exposed Persons	
5	Charities or other Not for Profit Organisations	
6	Sanctioned or other problematic customers	
7	Corruption slush funds	
8	MTIC/Carousel and/or other tax frauds	
9	Trade based money laundering incl TF	
10	Fraud	

Source: Author

Commercial banking is potentially vulnerable to and/or could be abused in a number of ways. Here are the top inherent ML related risks facing a commercial bank.

1. Customers with Cash Businesses

Customers that have businesses that deal in cash in large amounts, high value and/or with a large number of transactions are highly vulnerable to being used by money launderers as a vehicle to covert and launder the proceeds of crime. Slot machines within casinos or gambling houses were in part originally designed to take coins which were in those days equivalent to the cash notes earned today by criminals. Other coin intensive businesses like laundromats were also useful and attractive businesses for the criminal. There are few high value and/or retail businesses that couldn't be used though a few are considered particularly vulnerable and these include; high value goods dealers, for example, real estate agents; art dealers including (auctioneers); precious metals and stones dealers (including jewellers); car, plane and yacht dealers; watch dealers, equine or other high bred animal dealers; and cash intensive businesses including; retail outlets such as garages, restaurants, ice cream parlours, clubs (including strip bars) and bars, golf clubs, bowling alleys, private ATM companies, sauna and massage parlours and of course laundromats. There are some businesses that could fall into both categories and these include; money service businesses, both regulated and unregulated; jewellers; auctioneers and casinos. Banks may monitor aggregate cash or cash like activity, identifying unusually significant cash or cash like values and volumes and/or material changes and investigate material cases to identify whether there is satisfactory explanation or justification. Comparing customer businesses may also be useful in order to identify an outlier for further investigation. For more details on some of these businesses see Part 1, Section 2, Sub-section 2, Cash-Intensive Businesses, High Value Goods Dealers, Precious Metals & Stones Dealers and Real Estate Agents.

2. Customers with Sensitive Businesses

Other businesses accounts where cash is a large part of the activity may also present risks, particularly if they would not ordinarily be considered normally cash intensive, for example, embassy or consulate accounts. The following may also present risks: business accounts for arms dealer companies or private military firms; businesses that make and/or distribute war materials, in particular controversial weapons (nuclear, chemical or biological or cluster munitions and anti-personnel mines) or dual use goods may present additional risks, businesses involved in mining and minerals, particularly if involved in so called, mountain top removal, forestry

or logging businesses, particularly if involved in palm oil extraction leading to deforestation; businesses with poor human rights records or a record of environmental damage; businesses involved in waste management and scrap metal dealers and businesses that have been identified as posing increased corruption risks themselves, particularly when combined with increased country risks as set out in 3. below. For more details see Part 1, Section 2, Sub-section 1, Money Laundering Risks.

3. Businesses with Material Sensitive Country Risk Exposures

Customers, in particular customers with sensitive businesses that are based in or have material exposures to countries that have been identified as posing increased risks, for example countries the subject of sanctions and/or embargoes, with major corruption problems, organised crime and terror finance/WMD proliferation concerns. This also for customers owned or also time controlled by or dealing with sovereign governments and publicly owned entities from such countries, including Sovereign Wealth Funds and municipalities. For more details see Part 1, Section 1, Bribery & Corruption; Terrorism Finance & WMD Proliferation Finance and Part 1, Section 3, Sanctions & Embargoes.

4. Politically Exposed Persons

Businesses that are either owned or controlled by, or where the beneficial owner is Politically Exposed Person. For more details see Part 1, Section 1, Bribery and Corruption and Part 1, Section 2, Sub-section 2, Politically Exposed Persons.

5. Charities or other Not for Profit Organisations

Charities or other Not for Profit Organisations, which could be either supervised or effectively or insufficiently unsupervised that raise, store, move and/or use money for charitable and other humanitarian causes that are either subject to an applicable sanctions listing, or are otherwise identified by credible sources as connected and/or involved in terrorism finance. Organisations providing humanitarian or other similar relief have been used and abused in particular as fronts for Islamic terrorism financing. For more details see Part 1, Section 2, Sub-section 2, Charities and other Not for Profit Organisations.

6. Sanctioned or Otherwise Problematic Customers

Customers that are either subject to an applicable sanctions listing, or are otherwise identified by credible sources as may be connected and/or involved in criminal activity, including corruption, terrorism finance, WMD proliferation etc. Banks must be wary

in particular to screen customers, including corporates and businesses for example, against known terrorists and major criminals against lists of persons made available prior to opening of accounts and against payment flows through the bank. For more details see Part 1, Section 3, Sanctions & Embargoes.

7. Corruption Slush Funds

Business accounts that establish what looks like a so called, "slush fund." Whilst many bribes are demand led and could be considered extortion, that is no excuse for any business to pay a bribe for or in relation to a commercial contract. Nevertheless, otherwise legitimate businesses have paid bribes, and no doubt despite the criminality and the consequences some will continue to do so. Industries prone to bribes include public works contracts and construction, oil and gas, mining, real estate and property development. There are also real concerns over some contracts and dealings in the arms industry and with private military firms. It is unusual for a bribe to be paid directly or for it to be described as such or to be transparent and the use of intermediaries is common. It is also common for businesses that may consider making or facilitating bribes to have company money segregated from normal company funds or funds come from an already established "slush fund". In cases where companies have established a slush fund this has typically been outside the home country of the parent company, most often in an offshore centre or tax haven, with the funds being off-balance sheet or largely unaccounted for, and under the sole signature of a senior employee or even ex-employee. For more details see Part 1, Section 1, Bribery & Corruption, Part 1, Section 2, Sub-section 2, Arms Dealers, Intermediaries and Private Military Firms.

8. MTIC/Carousel and or other Tax Frauds

Businesses, particularly new small start up businesses, with individuals without a business track record or strong references that engage in export and import in and out of the EU in goods such as mobile phones, computer chips, cosmetics, precious metals and computer software or other easily portable goods which quickly then close down after large volumes and cross border payments are processed may be involved in MTIC/carousel Fraud. For more details see Part 1, Section 1, Fraud, Tax Fraud & Cybercrime.

9. Trade Based Money Laundering including Trade Finance

Business accounts that may indicate risks relating to Trade Based Money Laundering ("TBML"), including trade finance is practised to hide criminally derived proceeds and move value through the use of trade transactions in an attempt to legitimise

their illicit origins. TBML can be done through the misrepresentation of the price, quantity or quality of imports or exports and it can use techniques that vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail. The most common techniques of TBML are (i) over- and under-invoicing of goods and services (ii) over- and under-shipment of goods and services (iii) multiple invoicing of goods and services (iv) falsely describing goods and services on custom forms. The technique of over- and under-invoicing of goods remains a common method used to fraudulently transfer value across borders with the importer and exporter working in collusion together. Often the importer and exporter are part of the same corporate organisation, making the transfer even more difficult to detect. By invoicing the goods or service at a price below market price, the exporter is able to transfer value to the importer as the payment they will be required to make is less than the amount the importer will earn when the goods are sold in the market. Alternatively, by invoicing the goods or service at an above market price, the exporter is able to receive value from the importer as the payment for the goods or service is less than the value the importer will earn when it is sold in the market. Therefore, the over- and under-invoicing of exports and imports can have significant tax implications. An exporter who over-invoices the value of the goods they ship may be able to raise the amount of the export tax credit (or VAT rebate) they receive. It should be noted that in extreme situations, there may not be any goods shipped at all but collusion between parties to provide false documentation to customs agents and/or to banks. Therefore, banks may unwittingly be involved in such "phantom" shipments. The use of false descriptions can also be used in the trade of services such as financial advice, consulting services and market research. In June 2008 the FATF published a best practices paper titled Best Practices on Trade Based Money Laundering⁷ in which the red flags associated with TBML were listed. For more details see Part 1, Section 1, Fraud, Tax Fraud & Cybercrime. For Trade Finance see above, earlier in this section on Commercial Banking.

10. Fraud

Customers applying for and receiving credits or other financial assistance based on misrepresented facts and figures, either directly or through company account fraud or sinks. For more details see Fraud, Tax Fraud & Cybercrime in Part 1, Section 1.

Correspondent Banking

"US correspondent banking provides a significant gateway for rogue foreign banks and their criminal clients to carry on money laundering and other criminal activity in the US and to benefit from the protections afforded by the safety and soundness of the US banking industry."

US Senate Permanent Subcommittee on Investigations, Report, Correspondent Banking: A Gateway for Money Laundering 2001⁸

Introduction

As far back as 2001, there were some concerned that correspondent banking offered high risk foreign banks access to the US financial system by opening correspondent accounts at US banks or at foreign banks that already had a US correspondent bank account, that an investigation was conducted and a report issued by the US Senate Permanent Sub-committee on Investigations, entitled 'Correspondent Banking: A Gateway for Money Laundering.' It provided the inside story and a wake up call, focussing on the operations of ten foreign banks that had used major US banks to move and launder millions of dollars obtained through drug trafficking, financial frauds, bribes, tax evasion and illegal gambling operations.

Whilst much has certainly been done to improve standards both in the US and elsewhere, there remains concern that some of the underlying inherent vulnerabilities remain and that unless standards are maintained and AML Programmes are robust, correspondent banking will continue to be abused and criminals will take full advantage.

Definition/Description

Correspondent banking is the provision of banking-related services by one bank (correspondent) to another bank (respondent) often overseas to enable the respondent to receive deposits from, or make payments or other disbursements from that account with the correspondent, both for own correspondent and for the respondent's customers' cross border purposes that it cannot provide itself, typically due to a lack of an international network. Foreign financial institutions maintain correspondent accounts at domestic banks to facilitate international trade and investment by gaining access to the financial system and its products and services. The scope of a relationship and extent of products and services supplied will vary according to the needs of the respondent, and the correspondent's ability and willingness to supply them (sometimes dictated by the risk rating assigned to the respondent) but may include: cash management services, including deposit

accounts; international funds transfers; cheque clearing; payable through accounts; pouch activities; foreign exchange services; overnight investment accounts; loans and letters of credit, again for both the bank itself and for its customers which could also include other banks.

Whilst FATF does not define correspondent banking it does provide an entire Recommendation, now R.13⁹ to set out the "Additional Measures" stating that "Financial institutions should be required, in relation to cross border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to: (a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action; (b) assess the respondent institution's AML/CFT controls; (c) obtain approval from senior management before establishing new correspondent relationships; (d) clearly understand the respective responsibilities of each institution; and (e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

FATF also provide that: "Financial Institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks.¹⁰ Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks."

Whilst many states have individual statutory provisions applying the FATF R.13, much in the way they have for R.12 on PEPs, the USA Patriot Act,¹¹ S.312, is an example of where a State has set out in more detail the expectations on financial institutions in this respect. S.312 contains a provision requiring US financial institutions to apply enhanced due diligence when establishing or maintaining correspondent accounts of a foreign bank that is operating: (i) under an offshore license; (ii) in a jurisdiction found to be non-cooperative with international anti-money laundering principles; or (iii) in a jurisdiction found to be of primary money laundering concern under Section 5.311 of the same Act.

The Section also requires US financial institutions to take reasonable steps to: (i) conduct appropriate enhanced scrutiny; (ii) determine whether the foreign

bank itself offers correspondent accounts to other foreign banks (for example, payable through so-called nested accounts) and, as appropriate, identify such foreign bank customers and conduct additional due diligence on them; and (iii) identify the owners of such foreign bank, if its shares are not publicly traded.

Following the Patriot Act, the Wolfsberg Group issued its own Correspondent Banking Principles¹² in 2002 which were considered then good practice in dealing with correspondents, and in particular when it comes to due diligence and monitoring, supplementing these with Correspondent Banking FAQs in 2006. The Group is currently working on a further update expected to be published in 2013.

In June 2013 BCBS published a consultative document entitled "Sound Management of Risks related to Money Laundering and Financing of Terrorism" and in Annex 2 thereof listed a number of factors that should be considered in evaluating the risk of counterparty correspondent banks. The paper states that: "Banks that undertake correspondent banking activities should conduct an appropriate assessment of the ML/TF risks associated with correspondent banking activities and consequently apply appropriate CDD measure. Correspondent banks should gather sufficient information, at the beginning of the relationships and on a continuing basis after that, about their respondent banks to fully understand the nature of the respondent's business and correctly assess ML/TF risks on an ongoing basis. Factors that correspondent banks should consider include: the jurisdiction in which the respondent bank is located; the group to which the respondent bank belongs, and the jurisdictions in which subsidiaries and branches of the group may be located; information about the respondent bank's management and ownership (especially the presence of beneficial owners or PEPs), its reputation, its major business activities, its customers and their locations; the purpose of the services provided to the respondent bank; the bank's business including target markets and customer base; the condition and quality of banking regulation and supervision in the respondent's country (especially AML/CFT laws and regulations); the money laundering prevention and detection efforts of the respondent bank; a description of the CDD applied by the respondent bank to its customers; the identity of any third-party entities that will use the correspondent banking services; information on any possibility of a chain of correspondent banking and information on the AML/CFT policies and procedures may rely on any questionnaire filled by the respondent or on publicly available information provided by the respondent (such as financial or any mandatory supervisory information).

Money Laundering/Terrorist Financing Risks

Transactions through foreign correspondent accounts are typically large and permit movement of a high volume of funds relatively quickly. These correspondent accounts also provide foreign entities with ready access to international banking systems. These banks and other financial institutions may be located in countries with unknown AML regulations and controls ranging from strong to weak, corrupt, or nonexistent. A correspondent handling transactions which represent the proceeds of criminal activity or terrorist financing risks, may be subject to regulatory fines and/or damage to its reputation. For these reasons, correspondent banking is considered to be one of the highest risk products offered by a financial institution and financial institutions have to demonstrate that they have adequate processes and controls to recognise and manage the risk that it can be used for illicit activity.

The risks are well described by going back to the US Senate Permanent Subcommittee on Investigations, Report, Correspondent Banking: A Gateway for Money Laundering 2001 where the minority staff found that as at that time: (i) correspondent banking provides a significant gateway for rogue foreign banks and their criminal clients to carry on money laundering and other criminal activity in the US and to benefit from the protections afforded by the safety and soundness of the US banking industry; (ii) offshore banks, shell banks, and banks in jurisdictions with weak bank supervision carry particularly high money laundering risks, and US banks have routinely established correspondent relationships with such banks; (iii) most US banks do not have adequate anti-money laundering safeguards in place with respect to correspondent banking, and this problem is longstanding, widespread and ongoing; (iv) high risk foreign banks that are denied their own correspondent accounts at US banks can obtain the same access to the US financial system by opening correspondent accounts at foreign banks that already have a US bank account; and (v) in the last three years, some US banks have become concerned about the vulnerability of correspondent banking to money laundering and are taking some steps to reduce the money laundering risks, but the steps are slow, incomplete, and not industry-wide.

Based on its findings, the Minority Staff recommended that: (a) US banks should be barred from opening correspondent accounts with shell banks; (b) banks should be required to use enhanced due diligence and heightened anti-money laundering safeguards as specified in guidance or regulations issued by the US Treasury Department before opening correspondent accounts with foreign banks that have offshore

licenses or are licensed in jurisdictions identified by the US as non-cooperative with international anti-money laundering efforts; (c) banks should conduct a systematic review of their correspondent accounts with foreign banks to identify high risk banks and eliminate problem banks and should strengthen their anti-money laundering oversight; (d) banks should be required to identify a respondent bank's correspondent banking clients, and refuse respondent banks that allow shell foreign banks or bearer share corporations to use their US accounts; and (e) bank regulators and law enforcement officials should offer improved assistance to US banks in identifying and evaluating high risk foreign banks.

Whilst the report is US specific, its findings clearly applied elsewhere too, albeit the US Currency has always been the most popular currency amongst foreigners besides their own and likely also by criminals. Whilst much has been done including, shutting out shell banks, and restricting access to offshore banks, to improving bank AML Programmes across the board, little has been done to either identify non-co-operative foreign jurisdictions or to identify individual high risk foreign banks, although banks have internal risk based country models, and so some of these banks are likely still to be able to access the international financial system.

Out of all the activities conducted with correspondent banks and through or affecting the account, some possess much higher risks than others. For example, conducting proprietary activity of the other bank, perhaps trading and settlement, treasury and FX business, or fund execution and settlement can all be considered lower risk. At the other end of the risk spectrum are third party wire transfers, particularly payable through accounts and downstream clearing or so-called nested accounts, banknotes, precious metals and pouch services which are commonly offered as part of a correspondent banking relationship and involve the transmission and processing of monetary instruments, for example, money orders, traveller's cheques, and bank cheques.

As cross border wire transfers come under increased scrutiny and regulation, criminals have found paper cheques, money orders, and cashier's cheques to be an effective method to move money internationally. These more traditional payment instruments take a longer time to clear and be available for use but are perceived by money launderers as being subject to less scrutiny. Although wire transfers are used in many legitimate ways, most money launderers use wire transfers to aggregate funds from different sources and move them

through accounts at different banks until their origin cannot be traced. Despite being deemed as high-risk and subject to increased scrutiny, wire transfers are still frequently used in the layering stage of money laundering. Successive wire transfers allow the originator and the ultimate beneficiary of the funds to obtain relative anonymity, disguise the money trail, easily aggregate funds from a large geographic area, move funds out of or into a country, and legitimise illegal proceeds. The money launderers can also wire the funds to offshore accounts in countries with secrecy laws in place. It can be challenging for financial institutions to identify suspicious transactions due to the large number of wire transactions that occur in any given day.

Correspondent banking can generally be considered as having **high** inherent AML risks. The following are the top inherent money laundering risks for a correspondent bank.

Top ML Risks in Correspondent Banking	
1	Shell Bank Customers or Banks with Shell Banks as Customers
2	Offshore Banks
3	Non-Bank Financial Institutions, eg MSBs
4	Customers with Material Sensitive Country/ PEP Risk Exposures
5	Sanctioned or Other Problematic Customers
6	Group Companies, Parents, Subs and Affiliates
7	Wire Transfers
8	Payable Through Accounts
9	Pouch Services
10	Downstream Clearing/Nested Accounts
11	Banknote/Precious Metals Services
Source: Author	

1. Shell Bank Customers or Banks with Shell Banks as Customers

Shell bank customers are to be avoided, be it as direct or indirect customers of a bank. A shell bank means a bank that (1) does not conduct business at a fixed address in which it is authorised to conduct banking activities, (2) does not employ anybody on a full time basis at that fixed address, (3) does not maintain operating records at that address, (4) is not subject to inspection by the banking authority that licensed it to conduct banking activities. A post office box or electronic address is not a "fixed address" for these purposes.

2. Offshore Banks

Offshore banks are those banks that have a limited banking license that does not allow it to conduct business with citizens of, or in the local currency of, the country that issued the license. There are particular risks when dealing with a bank holding an offshore banking license as the jurisdiction in which it operates may have lax AML controls and standards or inadequate regulatory oversight. However, a proper assessment of the nature of an offshore license is necessary as not all will be of concern for example, as certain jurisdictions see an offshore licence as "a probation period" before banks can obtain an onshore licence. Offshore banks that are part of a banking group will generally present less risks.

3. Non-Bank Financial Institutions (for example MSBs)

Money Services Business and other non-bank financial institutions for example, remittance businesses, exchange houses and similar businesses such as those known as "Doleiros" and "Casa de Cambios" have long been identified as presenting risks for correspondent banks, whether providing direct banking accounts or indirect via downstream or nested accounts with banking correspondents (see below). Of course unregulated MSBs including, "Hawala", "Hundi", "Chop" etc. should be avoided if identified. For more details see Part 1, Section 2, Sub-section 2, Money Services Business.

4. Customers with Material Sensitive Country/PEP Risk Exposures

Customers, in particular bank customers, are based in or have material exposures to countries that have been identified as posing increased risks, for example, countries which are the subject of sanctions and/or embargoes, with major corruption problems, organised crime and terror finance/WMD proliferation concerns. Bank customers' client base and operations as well as ownership and domicile will also be relevant. This is also for customers owned or controlled by or having material connections with PEPs, for example, the PEP is either in a governing position or is to a significant extent the owner or controller of the bank customer or exerts significant influence. For more details see Part 1, Section 2, Sub-section 2, Politically Exposed Persons.

5. Sanctioned or Otherwise Problematic Customers

Bank customers that are either subject to an applicable sanctions listing, or are otherwise identified by credible sources as may be connected and/or involved in criminal activity, including corruption, terrorism finance or WMD proliferation etc. Banks must be wary to screen bank customers and transactions but also to identify

bank customers that have branches, or affiliates with a presence in or otherwise material business interests in so called sanctioned countries which may also be of concern. For more details see Part 1, Section 3, Sanctions & Embargoes.

6. Group Companies, Parents, Subs and Affiliates

Banking groups, particularly large international ones, will often offer correspondent banking accounts to other group companies but in so doing should not assume that such a relationship does not present similar risks to those offered by third party banks. Whilst parent banks may apply group wide standards and may have access to information about all group companies, some may not and beyond parents the same may not be able to be said for other group companies. As such intra-group bank customers should also be subject to a risk assessment, risk rating and appropriate due diligence and scrutiny.

7. Wire Transfers

There are a variety of methods for making payments from one party to another, from the most basic form of using cash, to issuing a cheque, to making payment with a debit or credit card, paying with a prepaid card to making a wire transfer between bank accounts. The same is true for international payments where most popular is the wire transfer, followed by the transfer of cash at a cash office such as Western Union, but international foreign currency cheques can also be used and available from a bank, where a person has an account, and increasingly especially with the rise of the Internet by the increased use of debit and credit cards. As payments from one currency to another will incur charges, there are also some more specialist services such as online currency brokers, that will make payments also, usually at better rates than those offered by Banks.

Although simple, sending cash through the post and particularly overseas isn't recommended, with some countries prohibiting sending cash in the post, the security concerns are obvious. As a result many people use Cash Transfer or Money Remittances Businesses, for example provided by companies such as American Express, Western Union and MoneyGram or by so called Casa De Cambios or FX Exchange Houses. An alternative could be a Prepaid card which can be purchased and loaded with an amount and shipped to the recipient with the PIN being communicated separately. International cheques are expensive and take time to ship and to clear, whilst credit and debit cards are good for low value amounts but not for higher amounts.

That leaves electronic or wire transfers. Wire transfers originated in the 19th century, sent over telegraph

lines. This process gave them their name wire as telegraphs were transmitted over wires. Bank wire transfers are often the cheapest method for transferring funds between bank accounts. A bank wire transfer is effected as follows: The entity wishing to do a transfer approaches a bank and gives the bank the order to transfer a certain amount of money. IBAN and BIC codes are given as well so the bank knows where the money needs to be sent. The sending bank transmits a message, via a secure system (such as SWIFT or Fedwire), to the receiving bank, requesting that it effect payment according to the instructions given. The message also includes settlement instructions. The actual transfer is not instantaneous: funds may take several hours or even days to move from the sender's account to the receiver's account. Either the banks involved must hold a reciprocal account with each other, or the payment must be sent to a bank with such an account, a correspondent bank, for further benefit to the ultimate recipient. Banks collect payment for the service from the sender as well as from the recipient. The sending bank typically collects a fee separate from the funds being transferred, while the receiving bank and intermediate banks through which the transfer travels deduct fees from the money being transferred so that the recipient receives less than what the sender sent.

Banks in the US use the CHIPS or Fedwire system to actually effect the payment. Domestic bank-to-bank transfers are conducted through the Fedwire system, which uses the Federal Reserve System. Other forms of electronic transfers include, for example, Electronic funds transfer system (EFTS). This is the system used when someone gives a bank account number and routing information to someone owed money and that party transfers the money from that account. It is also the system used in some payments made via a bank's online bill payment service. EFTS transfers differ from wire transfers in important legal ways. An EFTS payment is essentially an electronic personal check, whereas a wire transfer is more like an electronic cashier's check. In the United States, such EFTS transfers are often called "ACH transfers," because they take place through the Automated Clearing House. One important way ACH transfers differ from wire transfer is that the recipient can initiate it. There are of course restrictions, but this is the way people often set up automatic bill payment with utility companies, for example.

Banks in the UK use BACS and CHAPS. BACS is an electronic system that for many years has been used to process Direct Debits, direct credits and standing orders for UK banks, whereas CHAPS is a same-day UK domestic electronic transfer payments system.

Countries around the world will have their own systems similar to those in the US and the UK.

A telecommunications network, the Society for Worldwide Interbank Financial Telecommunications (SWIFT),¹⁵ is most often used to send messages with international wire transfers. The SWIFT network has been built by internationally active financial institutions and is currently available to just over 10,000 users from 212 countries. The Swift network is relied upon for the transmission of more than six billion messages annually and almost 20 million per day. Payment messages make up 49% of the total followed by securities with 44%, treasury 5.6%, trade 0.9% and others including to do with the system itself 0.3%. As far as regions are concerned EMEA has 67% of the total traffic, the Americas 20% and APAC 12.4%. The increasing complexity of the financial market and payments systems (of which SWIFT, owned by the institutions themselves, remains the largest) have resulted in vast numbers of individuals and entities seeking to use the framework to transmit funds around the world for personal, commercial and, on occasions, illicit purposes. It is not unusual for the person sending the funds (the remitter) to have an account with a financial institution that not only does not have a wide global presence but also does not have any form of direct commercial relationship with the bank holding the account of the individual or entity to whom the funds are being transmitted (the beneficiary). It may also be the case that the funds are being transmitted in a currency other than the local one in either jurisdiction and this will usually involve US\$ or € transactions.

Wire Transfers (SWIFT)	
Annual Messages	6bio
Average Daily Messages	20mio
Payment Messages	49%
Securities Messages	44%
System Messages	5.6%
Trade Messages	0.9%
EMEA Region	67%
Americas Region	20%
Asia Region	12.4%
Source: SWIFT 2012	

In recognition of this challenge, smaller institutions establish relationships with larger institutions which are better connected, trade in different currencies and can be used to form a chain through which the funds

can be passed from the remitter to the beneficiary. This chain, which can involve as few institutions as three or four but potentially many more, requires the exchange of messages and information detailing the amount to be moved, the destination from which and to which the funds are travelling and the details of both the remitter and the beneficiary in order to ensure that the correct financial postings can be made at each of the institutions involved. Institutions other than those associated with the remitter and the beneficiary pay fees to the intermediate institutions (and also the transaction framework provider, for example, SWIFT) for the privilege of using them to form the payment chain.

Whilst information in a wire is sufficient to ensure the payment is made from and to the right destination, the information is by necessity limited. Banks in the payment chain, other than the remitter, have no opportunity to perform due diligence on the individuals and entities for whom they are moving funds as their only direct contractual relationship is with the remitting financial institution. The intermediary institutions are therefore moving funds on behalf of their customers' customer, someone with whom they have no direct relationship and have no opportunity to review and decide whether or not to proceed. Despite this difficulty, financial institutions want and need to try and satisfy themselves that their customer, the remitting or beneficiary institution, has adequate processes and controls in place to ensure that appropriate due diligence and other checks have been conducted at the time the remitting individual or entity opened the account from which the funds are being moved. Financial institutions will also need to monitor and scrutinise transactions to identify suspicious or unusual transactions and to identify transactions to prevent sanction violations.

An area of particular concern was the perceived lack of transparency in the payments messaging systems and in particular concerns over the abuse of so called bank to bank or cover payments to hide true remitters from the payment chain and the manipulation of data in payments to hide, for example, the names of sanctioned parties so that payments could still be processed and correspondent bank's payment filter protection systems would be bypassed.

In 2007, US regulators approached a number of financial services industry groups, including the Wolfsberg Group, expressed their concerns about the abuse of Bank to Bank or cover payments and asked the industry to design a solution to the problem on the basis that they were the system specialists and that any system designed and implemented by the regulators

without consultation with the industry would present additional implementation challenges. Industry representatives then worked to develop a number of alternative proposals and consulted widely before settling on a solution that has fixed the problem, with implementation in 2009.

In addition, in order to address the issue regulators raised around deliberately omitting customer details in order to avoid detection and blocking of these payments, the Wolfsberg Banks, which together covered a significant amount of correspondent banking payments made worldwide, issued a message to all their correspondent banks reminding them that they should abide by new "Transparency Principles" which they were expected to do, in order to maintain accounts, and in particular to ensure that so called "wire stripping" was not undertaken.

8. Payable Through Accounts

A Payable Through Accounts ("PTA") is an account through which a bank may extend cheque writing privileges to its bank customers. PTAs have long been used in the US by credit unions (for example, for checking account services) and investment companies (for example, for checking account services associated with money market management accounts) to offer customers the full range of banking services that only a commercial bank has the ability to provide. Under an international PTA arrangement, a domestic financial institution opens a master checking account in the name of a foreign bank operating outside the domestic location. The master account is subsequently divided by the foreign bank into "sub-accounts" each in the name of one of the foreign bank's customers. Each sub-account holder becomes a signatory on the foreign bank's account at the domestic banking entity and may conduct banking activities through the account. While PTAs provide legitimate business benefits, the operational aspects of the account make it particularly vulnerable to abuse as a mechanism to launder money. Sub-account holders of the PTA master accounts at the domestic banking entity may include other foreign banks, rather than just individuals or corporate accounts. These second-tier foreign banks then solicit individuals as customers. This may result in thousands of individuals having signatory authority over a single account at a domestic banking entity. The PTA mechanism permits the foreign bank operating outside the domestic location to offer its customers, the sub-account holders, domestic currency denominated cheques and ancillary services, such as the ability to receive wire transfers to and from sub-accounts and to cash cheques. Cheques are encoded with the foreign bank's account number along with a numeric code to

identify the sub-account. Deposits into the domestic master account may flow through the foreign bank, which pools them for daily transfer to the domestic banking entity. Funds may also flow directly to the domestic banking entity for credit to the master account, with further credit to the sub-account.

9. Pouch Services

Pouch activity includes the use of a common carrier to transport currency, monetary instruments and other documents from a foreign country to a domestic bank account. Pouches can originate from an individual or another financial institution and can contain any kind of document, including all forms of bank transactions such as demand deposits and loan payments. The contents of the pouch are not always subject to search while in transport, and considerable reliance is placed on the financial institution's internal control systems designed to account for the contents and their transfer into the institution's accounts.

A prime benefit of having pouch services is the efficiency and speed with which international transactions can be deposited in another banking system by avoiding clearing a transaction through several international banks in order to move the funds abroad.

Pouch systems can be exploited by those looking for an avenue to move illegally-gained funds into another country in order to legitimise the proceeds and obscure the true source of the funds. Pouches are used to transfer bulk currency, both domestic and foreign and sequentially numbered monetary instruments. For instance, large dollar amounts can be transferred via pouch in the form of numerous cheques or money orders from various locations, with each payment below the reporting threshold. The payments are mailed or transported to accomplices overseas who deposit the cheques and other payments in foreign bank accounts. The foreign banks that receive them send them back for deposit in their correspondent accounts. The cheques and money orders are bundled up at the foreign banks and sent with a deposit slip with the details of each cheque and money order. The correspondent credits the Respondent's account and routes the individual payment instruments to the appropriate paying banks and other institutions.

Some banks handle millions of cheques a day delivered by shipping companies in pouches and overnight bags which makes it very difficult to aggregate related payments or scrutinise individual payments for evidence of money laundering. Once these illegal funds are deposited into the foreign correspondent accounts, they can be moved, mainly via wire transfer, anywhere in the

world.

10. Downstream Clearing/Nested Accounts

Foreign correspondent accounts provide clearing access to foreign financial institutions and their customers may include other foreign banks. High-risk foreign financial institutions have gained access to financial systems by operating through domestic correspondent accounts belonging to other foreign banks. These are commonly referred to as "nested" correspondent banks. Such nested correspondent bank relationships result in the financial institution's inability to identify the ultimate customer who is passing a transaction through the foreign correspondent's domestic account. These nested relationships may make it harder for the financial institution to effectively comply with due diligence standards, suspicious activity reporting, and economic sanctions monitoring.

11. Banknote/Precious Metals Services

Whilst not that common, it is possible to undertake precious metals and banknote services via correspondent banking accounts. Risks exist in particular, where physical settlement is involved in both cases. For more details see Part 1, Section 2, Sub-section 2, Precious Metals & Stones Dealers.

Credit & Other Cards

"You want 21% risk free? Pay off your credit cards"¹⁴
Andrew Tobias, American journalist, author and columnist

Introduction

Credit cards are based on the principle "buy now - pay later".

Credit cards developed from credit schemes applied by individual merchants, mainly gas/petrol stations, in the 1920s in the US, to sell gas/petrol to the growing population of car owners. This would lead to the development of credit cards with Diners Club in the 1950s being a consolidation of various different cards into one card which allowed the card holder to pay different merchants using only one card.

The first widely accepted plastic charge card was issued in 1958 by American Express, and the first general-use credit card that allowed balances to be paid over time was the BankAmericard (which in 1977 changed its name to Visa), issued in 1959.

In 1966, a number of banks formed the Interbank Card Association and in 1969, the Interbank Card Association bought the rights to use "Master Charge" from the California Bank Association. It was renamed MasterCard in 1979.

Today there are over 5 billion credit or other cards, with the US the biggest market with over a billion cards outstanding.

In addition, there were 354 million debit cards in use in 2006.

World's Largest Credit Card Companies by Outstanding in US\$bio

1	Bank of America/MBNA	194.70
2	Chase	184.09
3	Citi	148.90
4	American Express	105.00
5	Capital One	68.78
6	HSBC	58.50
7	Discover	49.60
8	Wells Fargo	36.40
9	Barclays	32.60
10	Lloyds TSB/HBos	19.29

Source: CreditCards.com¹⁵ and Nilson Report,¹⁶ December 2009 (through year-end 2009 and ranked by total worldwide outstandings)

Definition/Description

A credit card is a standard-size plastic card entitling the cardholder to use funds from the issuing financial institution up to the agreed limit. The cardholder may use the credit card to buy goods or services or withdraw cash from ATMs. When using the card the issuing company give the cardholder a loan which the card holder is usually expected to repay within 30 days. The credit limit is determined by the issuing card company based on the creditworthiness of the cardholder and can be lowered or raised at short notice.

A debit card or an ATM card operates in the same way as a credit card enabling the holder to buy goods and services and to withdraw cash from ATMs, however, the card will only allow transactions in so far as the linked or underlying account has a positive balance and no credit is therefore required.

A pre-paid card or stored value card does not have the credit facility feature. The value is either recorded remotely and linked to the card, or the value is stored on and accessible from the electronic chip built into the card. Stored value cards are also known as electronic purses. Pre-paid cards are usually issued in the name of the holder of the account to which the card is linked, whereas, stored value card are usually not linked to a name but like cash, are bearer and can be transferred and used by anyone holding the card.

Most General Purpose Credit Cards (in Circulation in 2008 in US\$)

1	Chase	119.4mio
2	Citi	92mio
3	Bank of America	80.2mio
4	Discover	48mio
5	American Express	46.5mio
6	Capital One	46.3mio
7	HSBC	38.8mio
8	GE Money	27.2mio
9	Target	23.4mio
10	Wells Fargo	17.3mio

Source: CreditCard.com¹⁵

According to Top10Reviews, the top 10 best prepaid

debit cards in the US were compared with an American Express card coming top. This card allows a maximum card balance of US\$2,500, a daily cash deposit limit of US\$500, no daily ATM cash withdrawal limit and no Daily Direct Deposit Limit. Out of all the top ten, two cards permit a maximum card balance of US\$15,000, with one of those cards, NetSpend Premier permitting a daily cash deposit limit of US\$7,500, daily ATM cash withdrawal limit of US\$940 and daily direct deposit limit of US\$7,500

Top 10 US Pre-Paid Cards	
1	American Express
2	Mango
3	Kaiku
4	NetSpend
5	AccountNow
6	Vision Premier
7	Green Dot
8	ACE Elite
9	READYdebit
10	Walmart MoneyCard

Source: Top 10 Reviews 2013 (prepaid-debit-cards-review.toptenreviews.com/)

Money Laundering/Terrorist Financing Risks

Cards may not, on the face of it at least, appear to be the primary financial product that would appeal to money launderers or those seeking to move funds on behalf of terrorist organisations but this is a perception that has started to change perhaps in reaction to forensic case analysis but also perhaps due to the fact that they were regarded as lower risk when compared to other products such as correspondent banking.

The same flexibility that forms a major feature of the "sales proposition" also potentially makes them attractive to launderers and terrorists although both groups recognise that the electronic payment framework and developed fraud detection systems make forensic evidence easier to obtain and near to "real time" intervention easier to undertake. That said, they do offer the ability to move funds across jurisdictional borders, using either an additional card which is issued to an individual in the second location or by physically sending the card together with the associated security details such as PIN information through the mail. This potential is recognised by card issuers and mirrors the activity that can often occur when cards are stolen or compromised and the fraudster attempts to put some

distance between the point of compromise and the point at which fraudulent activity is attempted.

The fact that there is such a close synergy between what a card issuer will be looking at in order to maintain a reasonable and appropriate fraud risk management framework and the things that a launderer might seek to use the card for, means that effective fraud control may also be a sound ML/TF suppressant.

Credit card fraud is a major problem, with 10% of US holders of credit cards and 7% of ATM or debit cards victims of fraud, with the average fraud being around US\$400 and estimates of the total amount of credit card fraud worldwide of US\$5.5bio. Of these frauds, 37% are counterfeit cards; 23% lost or stolen; 10% card not present (for example, giving card information to a non-legit telemarketer); 7% stolen cards during mail fraud and 4% identity-theft fraud.¹⁷

Beyond fraud, concerns have even been raised about Cards being used by terrorists, particularly suicide bombers. For example, spending undertaken in the direct period before a terrorist act may never appear on a statement prior to the event and so, in a rather macabre way, it is actually a way by which terrorists could fund their action in the short term at least. There is, however, a need for them to have been able to access the product in the first place, a process which usually requires them to have an established domicile and credit history. Recent events in the case of Al-Qaeda inspired individuals have sometimes been attempted by individuals who have only been radicalised after they have been resident and, in many cases, been working in the jurisdiction where the offence is committed and this requirement does not cause them a major problem. Another way in which card based products can be abused to launder funds is by having an additional card which is sent to someone in a second jurisdiction who withdraws funds and the bill is then settled by the primary card holder who remains in the original jurisdiction. The problem is that this can also mirror activity that is sometimes taking place for totally legitimate reasons, expatriates making funds available to their relations, for example, but most card issuers have recognised this risk and designed appropriate controls.

Equally interesting is the ever increasing use of pre-paid cards which tend to be either closed loop, where the card can only be used within a discrete set of outlets such as a shopping mall or particular company, or open-loop where access is available at any outlet supported by one of the major scheme issuers. The latter represents a more significant risk and most issuers of such products have controls to identify transaction

patterns that might indicate that the product is being abused. This can also be accompanied by controls restricting the total value of cash that can be used on the card during a set reporting period. The challenge is that these products are increasingly being used as an alternative to cash wage roll payments and are also attractive in some developing jurisdictions where they are seen as a halfway house between total cash usage and the adoption of credit based products which are difficult to price and risk model until there is sufficient operational knowledge and experience. It is stored value products that have been the primary focus for regulators and other interested parties and this has been reflected in two statements by the Wolfsburg Group. The first, dealing with credit cards,¹⁸ laid out the controls and risk assessments that it is appropriate for a financial institution to have in place and the second, on stored value cards,¹⁹ provided a detailed overview of how the products were designed and implemented as well as the associated controls. Both these publications, prepared by the Wolfsburg Group in association and conjunction with experts from other organisations, clearly outline the risks and provides a balanced assessment of what it is reasonable to expect a financial institution to be able to do.

Card based products are a data rich financial product where fraud prevention processes and procedures are well established and robust. These are supported by industry intelligence sharing and benchmarking but it does not mean that they are zero risk, rather that they continue to represent the lower end of ML/TF risk. The challenge is that they will continue to be refined and developed with an emphasis on added features, increased accessibility and an emphasis on low cost delivery. These factors mean that the attendant risk will continue to change and evolve and regular reviews will remain essential if a balanced and informed assessment of risk can continue to be made.

Credit and other card banking can generally be considered as presenting **low to moderate** inherent money laundering risks.

The main inherent money laundering risk for Cards is fraud.

Top ML Risks/Credit & Debit Card Fraud

Credit card fraud is the illegal obtaining of goods or services, or to obtain unauthorised funds from an account by using another persons credit card or any similar payment mechanism (for example, debit cards, store cards, etc.) as a fraudulent source of funds in a transaction. This can be done by creating a copy of a card, 'skimming' the details during a routine

transaction, stealing a card or intercepting it in the post and many other creative ruses. Credit card fraud is often committed in addition to identity theft. Counterfeit card fraud is undertaken using plastic cards that have been specifically produced or existing cards that have been altered. These cards are encoded with illegally obtained payment card account data in order to pay for goods and services or to withdraw cash. Card Not Present (CNP) fraud is committed using payment card account data to undertake transactions where there is no face-to-face contact between the seller and purchaser. Typically, this type of fraud is committed over the Internet, by mail order or telephone. CNP fraud is currently one of the fastest growing payment card related types of fraud. The most common examples of card fraud are the following:

Malware attacks: Malware is software that allows hackers access to the victims' computers. Undetected access allows them to steal passwords, bank information, and credit card numbers. Frequently updated anti-virus software keeps these attackers at bay.

Phishing and SMSishing: Phisher's pose as genuine businesses, such as banks or social networking sites. They send official looking e-mails and mobile text messages ("SMS") that prompt recipients to confirm passwords and account information.

Credit card skimming: Skimmers steal credit card information from legitimate transactions. Unsuspecting customers hand their credit card to a dishonest merchant, who uses a small skimmer device to read and store the credit card's number. The merchant then uses the information to purchase something, or sells the information to others.

Site cloning: Fraudsters might clone an entire website, or just the order form page of a merchant site. Victims enter all their information, including name, address, and credit card number, thinking they are making a valid purchase. They don't realise they are directing their ID to a thief.

False merchant sites: False sites easily dupe customers into providing their credit card information. They simply advertise their wares at ridiculously low prices, then request full credit card details from those who want to access the site.

Credit card generators: Using mathematical algorithms, this software imitates patterns of existing credit card numbers to create thousands of new credit card numbers. Many are actually valid numbers and expiration dates.

Investment Banking

"The reputation of a bank for integrity, generosity and thorough service is its most important asset, more important than any financial item. Moreover, the reputation of a firm is like a very delicate living organism which can be easily damaged and which has to be taken care of incessantly, being mainly a matter of human behaviour and human standards.... The basic conception of our firm has always been founded on the following principles: success from the financial and from the prestige point of view; important and self understood as it is, is not enough, what matters even more is a constructive achievement and adherence to high moral and aesthetic standards in the way in which we do our work"

Siegmund Warburg, founder of S.G Warburg & Co, acquired by UBS in 1995, from "The People's Banker"²²⁰ by Niall Ferguson

Introduction

Investment banking is described by its critics as casino banking and is in part responsible for the global financial crisis that began in 2007 and bankrupted two so called "Bulge Bracket"²²¹ firms in Lehman Brothers and Bear Stearns. If not for the intervention of governments around the world many more would have faced a similar fate. It was not the traditional investment banking businesses that were to blame, instead it was their proprietary trading activities that had come to dominate the industry, with investment banks behaving like large hedge funds.

Top 10 Investment Banks (US\$mio) by Fees		
1	JPMorgan	5,261.17
2	Bank of America Merrill Lynch	4,417.39
3	Goldman Sachs	3,8917.98
4	Morgan Stanley	3,527.09
5	Citi	3,417.13
6	Credit Suisse	3,216.74
7	Deutsche Bank	3,099.44
8	Barclays	2,966.35
9	UBS	2,061.56
10	Wells Fargo	1,814.50
Total		72,116.45

Source: FT.Com 2012

The distinction between proprietary trading and client or relationship focussed activities was already well understood in the 1960s during Siegmund Warburg's

rise. He preferred to distinguish what he espoused as constructive as "relationship banking", with what he termed, "transaction banking" which he described as "channelling big sums of money from certain quarters which had a surplus to certain other quarters where there was a scarcity of funds ... trading in money and of moving funds". According to Warburg, transaction banking, the preference for quantity over quality, had been one of the root causes of the Wall Street Crash and the Great Depression. The lesson of history, in his eyes, was that bankers should engage in advising firms they got to know intimately, rather than in speculation. "Personally," he wrote, "I am not interested in the waves of despondency and enthusiasm. These are appropriate for people who look upon matters purely from a stock exchange point of view ... However, if we want to succeed, we must make up our mind to follow a policy of establishing new values and new procedures rather than to act mainly as traders and sellers of securities which we find relatively easy to dispose of. In other words, we must be aware that we are primarily bankers and only secondarily stock exchange traders." With many in the investment banking industry, since Warburg's day, no longer speaking of "clients", but of "counterparties" and far from eschewing conflicts of interest, boasting instead of embracing and/or managing them, investment banking had travelled far from its core traditions, though there are signs that a return to these traditions is the way back to the future at least for some in the industry. It is clear that major investment banks are reconsidering the complexity of their business models and contemplating, with some even deciding upon, a far simpler strategy in the future. This may result in a return to the non-proprietary, client-centric model that Warburg espoused and would go some way to repairing the significant reputational damage suffered by the entire banking industry as a result of the financial crisis.

Definition/Description

An investment bank is a financial institution that assists individuals, corporations and governments in raising capital by underwriting and/or acting as the client's agent in the issuance of securities. An investment bank may also assist companies involved in mergers and acquisitions, and provide ancillary services such as market making, trading of derivatives, fixed income instruments, foreign exchange, commodities, and equity securities. There are two main lines of business in investment banking, 1) Trading securities for cash or for other securities (that is, facilitating transactions, market-making), largely with other financial institutions or the promotion of securities (that is, underwriting, research, etc. for clients, such as governments, institutions and companies, often known as the "sell

side"; 2) Advising those who manage assets (through mutual funds or hedge funds or pension funds or those who represent the investing public (who consume the products and services of the sell-side in order to maximise their return on investment) or run companies and businesses, constituting the "buy side". Many firms have both buy and sell side components. Securities can include all manner of different instruments. Where once trading and investing in government securities or debt dominated the markets, today instruments representing all manner of interests include: equities, fixed income, foreign exchange and commodities including precious metals. Financial derivatives can be issued and traded on the back of the markets in these instruments, for example, options, swaps, warrants, futures, or other structured products, sometimes called plain vanilla, for example, a simple option (that is, the right but not the obligation to buy at a certain price a fixed amount of a particular security at or within a certain time frame) or an exotic derivative, or more structured financially engineered, swapped, strangled and straddled packages of various different instruments. Securities and derivatives can be issued and traded on exchange on a regulated market with central clearing and settlement or Over The Counter ("OTC") on a bilateral basis between parties, as principal or as agent for customers. The derivatives market is significant (about US\$516 trillion in 2008) and experienced rapid growth through the late 1990s and early 2000s. Much has been written about the dangers of derivatives, especially the complexity and the risks. In 1988, the then Federal Chairman, Alan Greenspan stated, "what many critics of equity derivatives fail to realise is that the markets for these instruments have become so large not because of slick sales campaigns, but because they are providing economic value to their users."²²² Former SEC Chairman, Arthur Leavitt observed in 1995 that "derivatives are something like electricity; dangerous if mishandled, but bearing the potential to do good."²²³ It is not the derivative that is dangerous it is how they are used or perhaps abused, whether they are understood and appropriate in each case. The Global Financial Crisis of 2007 was a case in point. It was sparked from the bursting of the US housing bubble which had been fuelled by sub-prime Collateralised Debt Securities/Obligations (CDSs/CDOs) that pumped so much voltage into the housing grid that the system went into meltdown. Not only did these complex derivatives provide too much liquidity into the US sub-prime housing market, those holding the securities placed too much faith in their engineers and their own intellect and the securities failed to protect holders from huge losses despite the rating agencies confirming their ratings as AAA. As usual, one investor could at least say "I told you so" and more importantly avoid huge

losses as a result. In his 2002 Berkshire Hathaway letter to shareholders, company Chairman and CEO Warren Buffett expressed his concern with derivatives, referring to them as "weapons of mass destruction," a term popularised by George W. Bush to describe nuclear arms at the time. He stated that, "Unless derivatives contracts are collateralised or guaranteed, their ultimate value also depends on the creditworthiness of the counterparties to them. In the meantime, though, before a contract is settled, the counterparties record profits and losses—often huge in amount—in their current earnings statements without so much as a penny changing hands. The range of derivatives contracts is limited only by the imagination of man (or sometimes, so it seems, madmen)."²²⁴ His derogatory comments about derivatives appear to be directed toward those that create vast leverage and are involved in counterparty risk and perhaps come from his own experiences arising out of his 1998 acquisition of General Reinsurance Corp.²²⁵

An investment bank can also be split into private and public functions with an information barrier (also known as a 'Chinese Wall'²²⁶) which separates the two to prevent information from crossing. The private areas of the bank deal with information that may not be publicly disclosed, while the public areas such as stock analysis and traders deal with public information.

"Corporate finance" including, "mergers and acquisitions" is one of the core activities of an investment bank and is within one of the most important private sides of the bank, protected by informational barriers. Examples include; arranging an Initial Public Offering (IPO), a sale or placement of a block of shares, or a rights issue for a company client or a major corporate transaction such as a sale, merger or takeover.

Investment banks will also typically offer loans and extend credit to companies in order to facilitate capital market activity or simply to assist companies with their strategic goals. Syndicated loans are those offered by a group of investment banks working together to provide funds for a single borrower and the loan may involve fixed amounts, a credit line or a combination of the two. This spreads the risk of borrower default across multiple lenders. Syndicated loans can also be used as part of a leveraged buyout to fund large corporate takeovers with primarily debt funding. Unlike commercial banks, retail banks, or private banks, investment banks do not usually take deposits from the public and in fact, in the US, they were strictly not allowed to do so. From 1933 (Glass-Steagall Act) until 1999 (Gramm-Leach-Bliley Act), the US maintained a separation between investment banking and commercial banking due to

lessons learned from the Stock Market Crash of 1929 which led to the Great Depression of the 1930s. Whilst other industrialised countries, including G8 countries, historically had not maintained such a separation, the US as well as the UK and the EU are re-introducing firewalls and regulations to ring fence investment banking activities from deposits in banks once more, as the lessons from the 2007 global financial crisis are understood.

Money Laundering/Terrorist Financing Risks

Money laundering risks are usually those of a firm's customers, with the firm's employees being tasked with preventing and detecting any related suspicious activity. However, many of the biggest risks faced by investment banks include home grown ones. Much of these risks are exacerbated where there is a culture of reckless risk taking and individualism with high personal rewards the main incentives and an inadequate supervisory or effective control environment. Similar risks posed to an investment bank from its employees can also be presented by its customers, though the money laundering is not direct and the absence of knowledge should not cause the same direct damage to the firm.

Also investment banks rarely accept cash deposits or provide personal accounts that facilitate money transmission and/or third party funding that is not related to specific underlying investment transactions and so are generally seen as lower risk from a money laundering perspective. Terrorism finance appears to warrant little concern in investment banking. Whilst there were suggestions immediately after 9/11 that Al-Qaeda may have benefited in the financial markets ahead of the Attacks on America, no evidence was found and these suggestions have since been rejected.

Top ML Risks in Investment Banking	
1	Rogue / Unauthorised Traders
2	Insider Dealing by Employees
3	Market Manipulation by Employees
4	Bribery by Employees
5	Market Abuse by Customers
6	Sensitive Customers
7	Customers with Material Sensitive Country Risk Exposures
8	Politically Exposed Persons
9	Sanctioned or Other Problematic Customers
10	High Frequency-Algo Trading and Dark Pools

Source: Author

Investment banking can generally be considered as presenting **low to moderate** inherent money laundering risks, with the above being the top inherent risks facing an investment bank:

1. Rogue/Unauthorised Traders

Real risks can present themselves in the form of so called "Rogue Traders", going far beyond allowed position and trading limits and/or by employing fictitious schemes and devices which can expose the firm to excessive credit and market risks. The most recent is the case of Kweku Adeboli at UBS, (see Fraud section in Part 1, Section 1 and Criminal Cases in Part 2, Section 7 for Adeboli as well as other notorious Rogue Traders).

2. Insider Dealing by Employees

Beyond "Rogue Traders" investment banks need to be concerned with insider dealing by their employees. Investment banks are homes to significant amounts of inside information in their "Corporate Finance" departments and need to secure and protect this information, both from its own employees and from third parties who do not and should not have access to it. Whilst today there are few examples where information from behind a firm's Chinese Wall has leaked or been passed to the firm's trading side and acted upon for the benefit of the firm or for the individuals involved, there remain real reasons to be concerned that inside information is being shared more broadly and is being used by insiders, relatives and insider rings to profit illegally. For more details see Part 1, Section 1, Insider Dealing.

3. Market Manipulation by Employees

Market abuse and market manipulation are also real concerns to investment banks, particularly those ones with major trading operations. Looking out for improper schemes and malpractices remains an important task and these include the misuse of information such as front and parallel running, as well as other manipulative practices. For more details see Part 1, Section 1, Inside Information; Misuse of Information and Part 1, Section 1, Market Manipulation. Current concerns include rigging benchmarks, for details see Liber Bid Rigging Scandal in Part 2, Section 8, Enforcement Cases, but also investigations seem to have started beyond Libor and other interest rate benchmarks into precious metals and foreign exchange. In the Libor cases, illegal collusion between market participants have incurred the wrath of competition authorities in addition to that of regulators and to significant additional penalties.

4. Bribery by Employees

Whilst financial services has regularly appeared low

down relatively speaking on the lists of industries that are prone to corruption risks, the relative importance of emerging markets business to investment banks is growing as these markets and activity in these markets continue to outperform more established and developed markets. Corruption risks in relation to own deals is therefore likely to be increased and likely to increase further. Also, the use of third party intermediaries is a risk to be considered. Lavish entertainment or gifts may also be of concern. For more details on bribery and corruption see Part 1, Section 1, Bribery and Corruption and Part 2, Section 2, Sub-section 2, Intermediaries.

5. Market Abuse by Customers

Customers that indicate they could be operating a Boiler Room operation and/or other customers dealing in a manner raising concerns of market abuse, including insider dealing misuse of information and market manipulation. For more details see Part 1, Sections 1, Insider Dealing and Market Manipulation.

6. Sensitive Customers

Customers that could be involved in activity that is considered itself sensitive or controversial, for example, agreeing to manage funds from businesses such as; arms dealer companies or private military firms; businesses that make and/or distribute war materials, in particular controversial weapons (nuclear, chemical or biological or cluster munitions and anti-personnel mines) or dual use goods, businesses involved in mining and minerals, particularly if involved in so called, mountain top removal; forestry or logging businesses, particularly if involved in palm oil extraction or leading to deforestation; businesses with poor human rights records or a record of environmental damage; businesses involved in waste management; infrastructure and real estate funds. For more details see Part 1, Section 2, Sub-section 1, Money Laundering Risks Identified.

7. Customers with Material Sensitive Country Risk Exposures

Customers, in particular sensitive customers, that are based in or have material exposures to countries that have been identified as posing increased risks, for example, countries the subject of sanctions and/or embargoes, with major corruption problems and/or organised crime and terror finance/WMD proliferation concerns. This also applies to customers owned or controlled by or dealing with sovereign governments and publicly owned entities from such countries, including sovereign wealth funds and municipalities. For more details see Part 1, Section 1, Bribery & Corruption; Terrorism Finance & WMD Proliferation Finance and Part 1, Section 3, Sanctions & Embargoes.

8. Politically Exposed Persons

Customers that are either owned or controlled by, or where the beneficial owner is, a PEP. For more details see Part 1, Section 1, Bribery & Corruption and Part 1, Section 2, Sub-section 2, Politically Exposed Persons.

9. Sanctioned or Otherwise Problematic Customers

Customers that are either subject to an applicable sanctions listing, or are otherwise identified by credible sources as being connected and/or involved in criminal activity, including corruption, terrorism finance, WMD proliferation etc. Investment banks must screen customers, for example, against lists of known terrorists and major criminals prior to conducting business and against payment flows if to other parties. For more details see Part 1, Section 3, Sanctions & Embargoes.

10. High Frequency/Algo Trading and Dark Pools

The rise in high frequency trading and in particular algorithmic trading and trading using artificial intelligence is becoming a major part of the functioning of the securities markets and not just in equities but across many asset classes. Whilst these developments appear to provide increasing trading volumes and as a result improved market liquidity, lower trading costs, through reduction in bid ask spreads, resulting in a more efficient price discovery process which in theory should attract and encourage more investors, they also pose a threat. High frequency algorithmic trading by firms themselves and their clients could affect the stability of markets, which could provoke a serious downward spiral as happened for a time with the flash crash of May 2010, when American equity markets nosedived by almost 10% in the course of a few minutes, for example, as a result of a so called "errant algo" or by setting off sell orders en masse that take the markets quickly ever lower. The increases in liquidity provided by high frequency traders may well become illusory at times of market stress. The consequences for those involved if culpable and the damage done may be significant. Another concern is to some the unfairness in the market where high frequency traders gain an advantage over ordinary investors by putting their high powered servers right next to the exchanges data servers and so getting split millisecond advantages on the direction of the market which they use to make money, which has spawned an increase in Dark Pools off Exchange to hide from these traders, though Dark Pools are likely to become increasingly regulated and/or require to be more transparent.

Retail Banking

*"A bank is a place that will lend you money if you can prove that you don't need it."*²⁷

Bob Hope, American Comedian and Actor

Introduction

Retail banking is designed to provide individual customers with financial services for life, from college funding, to a regular chequing account, to credit and other card services, mortgages and loans, investments and insurance, to retirement trusts.

Much of the so called developed world's citizens have been able to readily access financial services, usually initially by opening an account relationship at a bank, as teenagers, expecting to hold on to their bank accounts until the day they die. This can be contrasted with many in other parts of the world where according to the World Bank,²⁸ still 2.5 billion people do not have access to banking services. With new technology, there is every reason to believe that the numbers without access to financial services will reduce significantly and at the same time, it is far from clear that banks will maintain their traditional dominance as the principal provider of retail financial services, particularly for those currently unbanked.

As banks continue to develop and offer products, to maintain the international payments system and work harder to defend their customer franchises, there is the risk that major new players emerge and replace banks as the principal customer interface and channel for tomorrow's financial services. In many places tomorrow's world is here today with mobile services taking off around the world and with many predicting the mobile phone and the mobile phone company challenging the banks in offering an alternative electronic purse and payment offering that is both competitive and compelling.

With customers being the lifeblood for retail banks, retaining customer loyalty in an environment where trust in banks is at a low level remains a challenge, though generally as the lack of trust appears to be an industry wide issue this is not translating into mass migrations of customers, and inertia seemingly also plays its part.

Definition/Description

A very large percentage of the population in developed and even developing countries that have bank accounts usually have their accounts at a retail bank. Today much of retail banking is streamlined electronically via

Automated Teller Machines (ATMs), or through virtual retail banking known as online banking. Ultimately, retail banking is designed to provide consumers with banking services for life, from college funds opened at the birth of a child to retirement trusts established to pay for old age.

Since so many people have bank accounts at retail banks and since the practice of laundering money can be a numbers game that favours the criminal, that is, the more accounts a financial institution has to monitor for money laundering and other suspicious activity the better the chances are for criminal proceeds to go undetected, retail banks can be an attractive place for money launderers. Therefore, retail banks are a popular type of financial institution for all three stages of the money laundering process, especially the first stage, the placement stage.²⁹

There are many products and services that retail banks provide to customers through brick and mortar branches, though much of retail banking is today streamlined electronically via ATMs, through virtual retail banking known as online banking, telephone banking, video banking and mobile banking.

The most basic retail banking services for individual customers include savings and checking accounts, safe deposit boxes, wire/journal services, access to wire transfer/payments services, home and car loans, certificates of deposit (CDs), retirement accounts, bill paying services, direct deposit services and debit and credit cards. For more details regarding cards, see Part 1, Section 2, Sub-section 3, Credit & Other Cards.

Although retail banking is, for the most part, mass-market driven, many retail banking products extend to small and medium sized businesses. For small businesses, the banking products include merchant and payments services, cash handling, insurance brokerage, and payroll and employee benefits services. For more details see Part 1, Section 2, Sub-section 3, Commercial Banking above.

Many large financial institutions or so called universal banks have a distinct and important "retail banking" business. Some retail banks are international corporations with numerous branches located across the globe, though most have a dominant home location. Others retail banks operate on a national level while smaller retail banks may be regional or have single branches. The following 15 banks that have some of the largest retail operations in their home countries and have grown overseas have an aggregate over 1 billion customers. Whilst more limited than banks an

alternative retail institution E-bay, for example, via its Pay Pal network has an estimated 232 million accounts albeit only 100 million are considered active.

Large (Country Champion) Banks by Customers

Bank	Home Market	Est No
Ag Bank of China	China	323mio
Citigroup	US	200mio
State Bank of India	India	125mio
HSBC	UK	95mio
Grupo Santander	Spain	90mio
Wells Fargo	US	70mio
Bank of America	US	57mio
Sperbank	Russia	55mio
Banco do Brasil	Brasil	55mio
Unicredit	Italy	40mio
Deutsche Bank	Germany	28mio
Nordea	Scandinavia	11mio
Nat Australia Bank	Australia	10.6mio
RBC	Canada	18mio
BNP Paribas	France	8.5mio
Standard Bank	South Africa	5.4mio

Source: Author 2013 (Guestimates)

Money Laundering/Terrorist Financing Risks

Whilst a third of the world's population do not have access to bank accounts or financial services, and the best estimate of funds laundered in 2009 is US\$1.6 trillion³⁰ or 1.5% of global GDP, it can be safely assumed that the overwhelming amount of funds within banks and, in particular in retail banks, is of little concern from a money laundering and terrorist financing perspective.

That being said, whilst retail banks handle high volumes of cash and cheque deposits and cash withdrawals, wire transfers to other financial institutions, between accounts and other high volume activity, there remains a risk that such transactions will include the proceeds of crime or may be used to fund terror activities, noting for the latter in particular, the relatively small amounts needed to carry out acts of terror. Retail banking is often a customer's first point of entry into a bank and so establishing effective controls from the outset is imperative.

Retail Banking can generally be considered as presenting **moderate to high** inherent money laundering risks and

the following are the top inherent money laundering risks for a retail bank. For many retail banks they also combine the commercial bank and so in such cases these can be read together, but for this purpose the following relates to individual customers only.

Top ML Risks in Retail Banking

1	Customers with Cash Transactions
2	Customers with Material Sensitive Country Risk Exposures
3	Complex or Complicated Non Transparent Customers
4	Sanctioned or Other Problematic Customers
5	Credit and Loan Fraud
6	Identity Theft and Account Takeover
7	Tax Evasion
8	Credit Card and other Card Fraud
9	Bank Robbery
10	New Payment Methods

Source: Author

1. Customers with Cash Transactions

Cash deposits (including cash like, for example, cheques) can present a heightened risk for retail banks. Still banks are very aware of the risks of cash, especially large deposits and withdrawals; numerous deposits, concentration and then wiring out of the bank, including to third parties or overseas. Banks can be prone to smurfing in particular, where smaller deposits are made into various branches of the same bank to avoid the immediate detection of large value transactions.

2. Customers with Material Sensitive Country Risk Exposures

Customers, in particular sensitive customers, that are based in or have material exposures to countries that have been identified as posing increased risks, for example countries the subject of sanctions and/or embargoes, with major corruption problems, organised crime and terror finance/WMD proliferation concerns. For more details see Part 1 Bribery & Corruption; Terrorism finance & WMD Proliferation Finance and Part 4 Sanctions & Embargoes.

3. Complex or Complicated Non-Transparent Customers

Customers, that are unduly or excessively complex, where identification and/or due diligence is difficult to establish or carry out satisfactorily, for example

Customers operating through personal investment companies or numerous layers of holding vehicles which appear designed to hide the ultimate beneficial owner. Retail banking is a mass consumer business and as a result will generally not involve close relationship management by a named relationship manager.

Increasingly customers will interact with their bank through various channels, in person perhaps, though also perhaps not, as in some cases with telephone, online and mobile banking, the customer may not physically interact with the bank at all and so since there is no interaction with employees of the bank and their activity is rarely questioned unless the bank's monitoring systems catch the suspicious or abnormal activity, money launderers may seek to exploit such vulnerabilities.

4. Sanctioned or Otherwise Problematic Customers

Customers that are either subject to an applicable sanctions listing, or are otherwise identified by credible sources as may be connected and/or involved in criminal activity, including corruption, terrorism finance, WMD proliferation, etc. Banks must be wary in particular to screen customers, for example against known terrorists and major criminals against lists of persons made available prior to opening of accounts and against payment flows if to other parties.

5. Credit and Loan Fraud

Customers applying for and receiving credits or other financial assistance based on misrepresented facts and figures, either directly or through company account fraud or sinks. Whilst the most obvious risks are mortgage and other credit frauds, which for more details see Fraud in Part 1, Section 1 above, and credit card fraud, which for more details see Credit & other Cards in Part 1, Section 2, Sub-section 3, credits can be used as part of a money laundering scheme beyond fraud. Whilst credits and loans result in a borrower receiving money from the bank, this product can be used as part of a money laundering scheme, with the main money laundering risk arising through the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination. When loans are made in one jurisdiction, and collateral is held in another, this may also indicate a heightened money laundering risk.

6. Identity Theft and Account Takeover

With around two thirds of the world's population having access to retail bank accounts, and more on the way, banks are obliged to collect and copy identification documents, verified by still more documents in order to establish that the bank customer is not only who he purports to be but also that he is not, in fact, someone

the bank either should not or does not want to deal with, this despite the fact that identification documents are not hard to come by, particularly for those professional and/or organised criminal gangs. Identity theft and account takeover are a growing problem. For more details see Part 1, Section 1, Fraud including Tax Fraud and Cybercrime.

7. Tax Evasion

Customers that are non resident for tax purposes, may use a retail account to hold even small sums undeclared for tax purposes. A bank should never assist a customer in cheating its taxes, and if it becomes aware or suspects that a customer is cheating on its taxes, then it should, where tax crimes are predicate offences to money laundering, file appropriate suspicious activity reports.

8. Credit Card and other Card Fraud

For more details see Part 1, Section 2, Sub-section 3, Credit & Other Cards.

9. Bank Robbery

Retail branches hold large quantities of cash and of course carry a risk of robbery. Since formalised branches developed, security in this field has been increasing in effectiveness and it would be fair to say that bank robberies are a lower risk compared to what they once were. However, for successful bank robberies 80% of stolen money is never recovered. With most branches having standardised layout and features, it is not difficult to see why a bank may be an attractive source of cash. For more details see Theft, Robbery & Trafficking above in Part 1, Section 1.

10. New Payment Methods

Innovation has been a constant theme driving banking throughout the ages, with the 20th century being the century which brought numerous new modern products and services and new delivery channels to customers. With the first credit and charge cards being issued in the US in the 1950s see Part 1, Section 2, Sub-section 3, Credit and other Cards and the first ATM machine being installed by Barclays Bank in London in 1967. Today there are more than 1.6 million cash machines worldwide.

The ATM³¹ was invented by John Shepherd-Barron a UK inventor who supposed that there must be a way to get at his own money in the bank at any time anywhere in the world or the UK and he hit upon the idea of a chocolate bar dispenser, but replacing chocolate with cash. He pitched the idea to Barclays, who convinced them immediately. Mr Shepherd-Barron's machine used cheques that were impregnated with carbon 14, a mildly radioactive substance. The machine

detected it, then matched the cheque against a PIN number. These cheques would soon be replaced with Plastic Cards. The machine paid out a maximum of £10 a time. The first machines were vandalised, and one that was installed in Zurich in Switzerland began to malfunction mysteriously as it was later discovered that the wires from two intersecting tramlines nearby were sparking and interfering with the mechanism. One by-product of inventing the first cash machine was the concept of the PIN number. Mr Shepherd-Barron came up with the idea when he realised that he could remember his six-figure army number, but to be safe he decided to stick with a four digit number. Despite the success of his ATM machine, Mr Shepherd-Barron believes its use in future will be very different, predicting the demise of cash in many societies and predicting along with many others that electronic purses in the form of mobile phones could soon be ubiquitous, with a swipe of a phone at till points enough for small transactions, that are today settled with cash or a credit or charge card.

Mobile phone banking is seen by many as a solution to many in the developing world who do not have access to bank services, relying on money service business and informal operations but also to many in the developed world who increasingly receive and rely on the mobile phone and its "apps" for many and varied services. The portability, reliability and usability of smart phones make them a natural product to act also as an electronic purse. They also appear likely to supplement and in some cases supplant the take up of banking by other channels, for example, telephone and internet banking the latter, still suffering from concerns over internet security, which is likely to be a problem also for mobile phones but interestingly is not perceived quite as such by customers. Since 9/11 however, the FATF and member countries have become concerned that new payment methods could be used by money launderer's and terrorist financiers to circumvent money laundering controls established for the formal financial sector and in particular those applicable to banks and other non-bank financial institutions. Nevertheless, it is clear that the implementation of controls and design features can reduce risks and vulnerabilities, for example, imposing purse limits, usage controls, and systems to detect suspicious activity contributes to mitigating these risks. Furthermore, where the use of electronic purses is limited to small value payments, the use of this product is less attractive to would-be launderers. For terrorist financing, and other financial crime, electronic money offers a more accountable, and therefore less attractive means of transferring money compared to cash, provided KYC/AML checks are required. Still most electronic money products in commercial use

today do not provide the kind of privacy or anonymity that cash provides, nor its utility. This is due to a number of factors: commercial practice, for example, dictates that most products are funded by payments from bank accounts or credit cards, and therefore can often reveal the identity of the customer at the outset, or at least such customers have been taken on and screened. Similarly, use of these products often leaves an electronic trail that can help locate, if not identify, the user of a particular product. As issuers of electronic money usually occupy the position of intermediary in the payment process, situated between two financial or credit institutions, they are often able to provide additional transaction information to law enforcement investigations that complements identity data provided by other financial institutions. This may be equally or more valuable in the chain of evidence than a repetition of the verification of identity process, as it can yield valuable information to assist law enforcement in that event. Fraud prevention and consumer protection concerns led to the placement of transaction, turnover, and purse limits on products, limiting the risk to both issuer and consumer. These limits act to restrict the usefulness of the product for money laundering, and make unusual transactions more detectable.

Of course where controls or missing or design features apply to increase the risks, this is possible, for example, the higher the value and frequency of transactions, and the higher the purse limit, the greater the risk: The €15,000 threshold for occasional transactions provided in the Regulations may in this context provide a convenient comparator when assessing such risk; Frequent cross-border transactions, unless within a single scheme, can give rise to problems with information sharing; Dependence on counterparty systems increases the risk; Some merchant activity is particularly susceptible to money laundering, for example, betting and gaming offer a number of opportunities either with or without the collusion of the merchant; and money service businesses are considered as susceptible to exploitation for money laundering and terrorist financing; Funding of purses using cash offers little or no audit trail and hence presents a higher risk of money laundering; The non face-to-face nature of many products also gives rise to increased risk; The ability of consumers to hold multiple purses (for example open multiple accounts or purchase a number of cards) without verification of identity increases the risk; Redemptions at ATMs, as well as any allowances for the payment of refunds in cash for purchases made using electronic money will also increase the risk; The ability of non-verified third parties to use the product increases the risk; and The technology adopted by the product may give rise to specific risks that should be assessed.

Wealth Management / Private Banking

"What makes private banking appealing to legitimate customers also makes it particularly inviting to criminals.... the Subcommittee found that in several cases criminals used private banking services to move huge sums of money with the assistance of private bankers....In essence, private bankers act like a concierge at an expensive hotel."

US Senator Susan Collins - 1999 Permanent Subcommittee on Investigations' "Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities"³²

Historically, private banking developed in Europe. Some banks in Europe are known for managing assets of some royal families.

The assets of Princely Family of Liechtenstein is managed by LGT Bank (founded in 1920). The assets of Dutch Royal Family is managed by MeesPierson (founded in 1720). The assets of British Royal Family is managed by Coutts (founded in 1692). Some American banks that specialise in private banking date back to 19th century, such as US Trust (founded in 1812) and Northern Trust (founded in 1889).

The country notable most for private banking is Switzerland, which remains the largest offshore centre, with about 27% (US\$2.0 trillion) of global offshore wealth in 2009, according to Boston Consulting Group.³³

According to the 15th annual World Wealth Report, by Merrill Lynch Global Wealth Management and Capgemini 2011 the population of High Net Worth Individuals ("HNWIs") increased to 10.9 million and HNWI financial wealth reached US\$42.7 trillion.³⁴

The US is still home to the single largest high net worth individuals' segment in the world, with its 3.1 million HNWIs accounting for 28.6% of the global HNWI population.

The global HNWI population remained highly concentrated in the US, Japan and Germany, which together accounted for 53.0% of the world's HNWIs. Asia-Pacific HNWIs' wealth was second as far as regions were concerned with US\$10.8 trillion, exceeding Europe's HNWI wealth of US\$10.2 trillion.

Top 20 Largest WM/PBs by Assets			
Rank	Bank	Country	(US\$bio)
1	UBS	CH	1,705
2	Bank of America	US	1,673.5
3	Wells Fargo	US	1,400
4	Morgan Stanley	US	1,308
5	Credit Suisse	CH	854.6
6	Royal Bank of Canada	Canada	628.5
7	HSBC	UK	398
8	Deutsche Bank	Ger	387.3
9	BNP Paribas	France	346.9
10	Pictet	CH	322.2
11	JPMorgan Chase	US	318
12	Citi Private Bank	US	250
13	Goldman Sachs	US	240
14	ABN AMRO	NL	212.7
15	Barclays	UK	201.4
16	Julius Baer	CH	200.8
17	Northern Trust	US	197.7
18	BNY/Mellon	US	179
19	Lombard Odier & Cie	CH	175.5
20	Santander	Spain	172.7

Source: Scorpio Private Banking Benchmark 2013³⁵

Definition/Description

Private Banking is the provision of banking and brokerage and investment services in a closely managed relationship to HNW clients.

Private banking targets only the very wealthiest clients or HNWIs, broadly speaking, those with more than around US\$1mio in investable assets, excluding primary residence, collectibles, consumables and consumer durables. Ultra-HNWIs are defined as those having investable assets of US\$30mio or more, again excluding primary residence, collectibles, consumables and consumer durables. Wealth management, by contrast, targets clients with assets in excess of US\$100,000, that is, affluent as well as HNW clients.

Such services will include bespoke product features tailored to a client's particular needs and may be provided from a wide range of facilities available to the client including: current account banking, high value transactions, use of sophisticated products, non-standard investment solutions, business conducted

across different jurisdictions, offshore and overseas companies, trusts or personal investment vehicles.

According to the S.312 of the US Patriot Act,³⁶ a "private banking account" is an account (or any combination of accounts) maintained at a bank that satisfies all three of the following criteria: (i) requires a minimum aggregate deposit of funds or other assets of not less than US\$1mio; (ii) is established on behalf of or for the benefit of one or more non-US persons who are direct or beneficial owners of the account; and (iii) is assigned to, or is administered by, in whole or in part, an officer, employee, or agent of a bank acting as a liaison between a financial institution covered by the regulation and the direct or beneficial owner of the account.

Private banks and wealth managers focus on a client's need and risk appetite, and tailoring the solution accordingly. Most modern private banks follow an open architecture product platform, offering suitable third party best in breed products. Still proprietary products and services are also offered, though increasingly it is the service the bank offers in sifting through the investment opportunities available and tailoring these to particular individual circumstances and preferences that marks the more successful operations. The offering will also include access to investment opportunities across all major asset classes and geographies and to reliable execution. Of course private banking customers will pay for these services, and the charges vary. There are private banks that follow the transactional model where the client is charged per transaction and others where advisory fees are charged. There are other private banks that follow a hybrid model. In this model, the bank charges a fixed fee for certain products and an advisory fee for the rest. The most recent industry trend is towards the advisory fee model, because margins on commissions may go down in the future.

Money Laundering/Terrorist Financing Risks

Whilst it was at one time thought that there were few money laundering risks in the private banking sector because of the personal contact between relationship managers and their wealthy customers, it was the release of a report and hearings by the US Senate Permanent Sub Committee on Investigations: 'Private Banking and Money Laundering: A Case study of Opportunities and Vulnerabilities 1999', that revealed major risks and concerns. Since that time, much has changed in the regulation and operation of private banking but the facts and concerns raised in that report remain important and in particular the case histories relating to amongst others *Abacha*, *Bongo*, *Salinas* and *Zardari* and their relationships with Citibank. For details see Part 2,

Section 7, Criminal Cases.

Money laundering risks can vary significantly between different private banks depending on their business models. Some private banks operating at the lower end of the risk 'spectrum' had businesses that was closer to that seen in a standard retail and investment businesses environment. At the higher end of the risk spectrum, firms provided services to a more internationally diverse client base, some of whom were located in high-risk jurisdictions, through advisors based across the globe. Customers of these firms were more likely to have non-standard financial requirements and manage their affairs through complex structures, a significant risk factor in itself.

According to FSA Peer review³⁷ - the following are the risk factors that are likely to increase the risk of money laundering within private banking businesses: an international customer base which includes people or organisations from jurisdictions with: a) relatively weak legal structures and/or economies, from which residents are likely to 'shelter' funds overseas; b) a reputation for providing secretive or discrete company and trust formation and administration services; and c) a poor record on the implementation of measures to prevent and enforce against financial crime, including corruption.

UK JMLSG Guidance Notes³⁸ state that money launderers are attracted to private banking by 'the availability of complex products and services that operate internationally within a reputable and secure wealth management environment that is familiar with high value transactions'. The following are examples cited by the JMLSG Guidance as factors contributing to the increased vulnerability of wealth management: a. wealthy and powerful clients, who may be reluctant or unwilling to provide adequate documents, details and explanations; b. multiple and complex accounts – within the same firm or group, or with different firms; c. cultures of confidentiality; d. concealment , for example, of beneficial ownership through offshore trusts; and e. countries with statutory banking secrecy in certain jurisdictions. f. movement of funds – often high value and rapid transfers. g. credit – the extension of credit to clients who use their assets as collateral also poses a money laundering risk unless the lender is satisfied that the origin and source of the underlying asset is legitimate.

Private banking services can be vulnerable to money laundering schemes and past money laundering prosecutions have demonstrated that vulnerability. The 1999 Permanent Sub-committee on Investigations

"Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities" outlined, in part, the following vulnerabilities to money laundering: a) private bankers as client advocates; b) powerful clients including politically exposed persons, industrialists, and entertainers; c) culture of confidentiality and the use of secrecy jurisdictions or shell companies; d) private banking culture of lax internal controls; e) competitive nature of the business; and f) significant profit potential for the bank.

Whilst private banking, particularly international private banking, is vulnerable to money laundering, the close relationship that private banks aim to have with their clients, and the bespoke requirements that many private banking clients have, should allow private banks to develop a very good understanding of their clients and the reasons for their clients' transaction activity. With this knowledge, the risks inherent in the business can be mitigated. In order to mitigate the risks banks should establish a risk profile for each customer to be used in prioritising oversight resources and for ongoing monitoring of relationship activities. The following factors should be considered when identifying risk characteristics of private banking customers: nature of the customer's wealth and the customer's business: (i) the source of the customer's wealth; the nature of the customer's business; and the extent to which the customer's business history presents an increased risk for money laundering and terrorist financing. This factor should be considered for private banking accounts opened for PEPs; (ii) purpose and anticipated activity: the size, purpose, types of accounts, products and services involved in the relationship, and the anticipated activity of the account; (iii) relationship: The nature and duration of the bank's relationship (including relationships with affiliates) with the private banking customer; (iv) customer's corporate structure: Type of corporate structure (for example, IBCs, shell companies (domestic or foreign), or PICs); (v) geographic location and jurisdiction: the geographic location of the private banking customer's domicile and business (domestic or foreign); the review should consider the extent to which the relevant jurisdiction is internationally recognised as presenting a greater risk for money laundering or, conversely, is considered to have robust AML standards; and (vi) Public information: information known or reasonably available to the bank about the private banking customer. The scope and depth of this review should depend on the nature of this relationship and the risks involved.

Wealth management/private banking can generally be considered as presenting **moderate to high** inherent money laundering risks and the following are the top

inherent money laundering risks for a wealth manager/private bank.

Top ML Risks in WM/PB	
1	Customers with Cash Transactions
2	Customers with Cash Businesses
3	Customers with Sensitive Businesses
4	Customers with Material Sensitive Country risk exposures
5	Complex or Complicated Non-Transparent Customers
6	Politically Exposed Persons
7	Sanctioned or Other Problematic Customers
8	Fraud including Market Abuse
9	Tax Evasion
10	Employees

Source: Author

1. Customers with Cash Transactions

Cash deposits (including cash like, for example cheques), particularly large cash deposits but also withdrawals can present a heightened risk for private banks. Though banks are very aware of the risks of cash, especially large deposits and withdrawals; numerous deposits, concentration and then wiring out of the bank, including to third parties or overseas.

2. Customers with Cash Businesses

Customers that have businesses dealing in cash in large amounts, high value and/or with a large number of transactions are vulnerable to being used by money launderers as a vehicle to convert and launder crime proceeds. There are few high value and/or retail businesses that could not be used though a few are considered particularly vulnerable including; high value goods dealers, for example, real estate agents; art dealers including (auctioneers); precious metals and stones dealers (including jewellers); car, plane, yacht dealers; watch dealers, equine or other high bred animal dealers; and cash intensive businesses including; retail outlets such as garages, restaurants, ice cream parlours, clubs (including strip bars) and bars, golf clubs, bowling alleys, private ATM companies, sauna and massage parlours and laundromats. Customers owning such businesses may further wish to launder or invest criminal proceeds. For more details on some of these businesses see Part 2, Section 2, Sub-section 2, Cash-Intensive Businesses, High Value Goods Dealers, Real Estate Dealers and Precious Metals and Stones Dealers.

3. Customers with Sensitive Businesses

Customers involved in arms dealing or in private military firms; customers involved in making and/or distributing war materials or dual use goods may present additional risks. Customers involved in mining and minerals, particularly if involved in so called, mountain top removal, forestry or logging businesses, particularly if involved in palm oil extraction leading to deforestation; businesses with poor human rights records or a record of environmental damage; Customers involved in waste management and scrap metal dealers and businesses that have been identified as posing increased corruption risks themselves, particularly when combined with increased country risks, including Intermediaries as set out in 3. below. For more details see Part 2, Section 1 Money Laundering Risks Identified.

4. Customers with Material Sensitive Country Risk Exposures

Customers, in particular sensitive customers, that are based in or have material exposures to countries that have been identified as posing increased risks, for example, countries the subject of sanctions and/or embargoes, with major corruption problems, organised crime and terror finance/WMD proliferation concerns. For more details see Part 1, Bribery & Corruption; Terrorism Finance & WMD Proliferation Finance and Part 3, Sanctions & Embargoes.

5. Complex or Complicated Non-Transparent Customers

Customers, that are unduly or excessively complex, where identification and/or due diligence is difficult to establish or carry out satisfactorily, for example customers operating through personal investment companies or numerous layers of holding vehicles which appear designed to hide the ultimate beneficial owner. For more details see Part 1, Section 2, Sub-section 2, Gatekeepers. Wealth management/private banking is not a mass consumer business, quite the opposite and should involve a close relationship with a named relationship manager where complexity is not uncommon in customer structures, though in any event the relationship manager must understand both the structure and the owners and controllers of the funds. If safe-deposit facilities are offered these should only be maintained for existing customers.

6. Politically Exposed Persons

Customers who are PEPs. For more details see part 1 Bribery and Corruption and Part 2, Section 2, Sub-section 2, Politically Exposed Persons.

7. Sanctioned or Otherwise Problematic Customers

Customers that are either subject to an applicable sanctions listing, or are otherwise identified by credible sources as may be connected and/or involved in criminal activity, including corruption, terrorism finance, WMD proliferation etc. Wealth managers/private bankers must be wary in particular to screen customers, for example against known terrorists and major criminals against lists of persons made available prior to opening of accounts and against payment flows if to other parties. For more details see Part 1, Section 3, Sanctions & Embargoes.

8. Fraud including Market Abuse

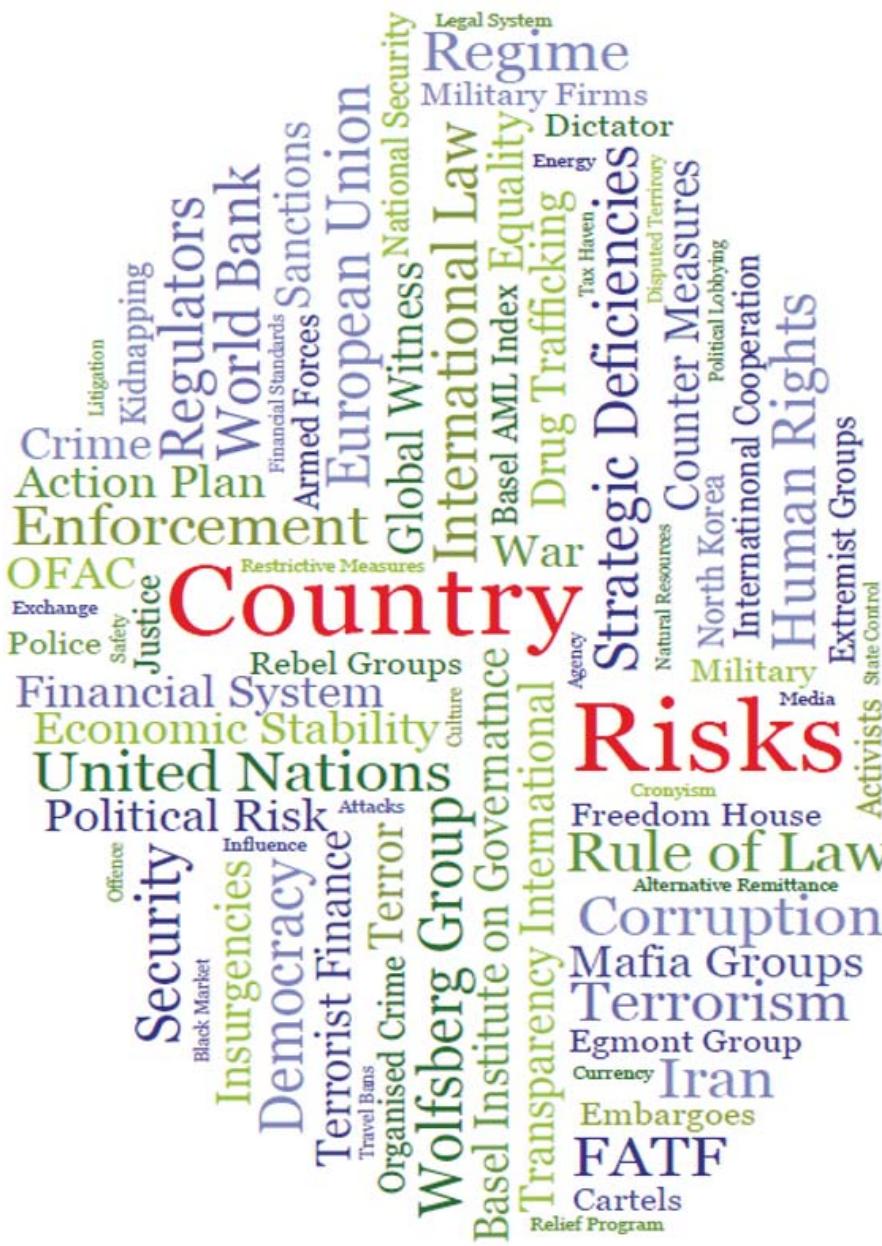
Customers that indicate they could be operating a Boiler Room operation and/or other customers dealing in a manner raising concerns of market abuse, including insider dealing misuse of information and market manipulation. Customers that are themselves insiders may present risks in some circumstances. For more details see Part 1, Section 1, Fraud; Insider Dealing and Market Manipulation.

9. Tax Evasion

Customers that are non resident for tax purposes, may use a private banking account to invest sums undclared for tax purposes and use the services of the brokerage to hide these investments. A bank should never assist a customer in tax evasion, and if it becomes aware or suspects that a customer is evading taxes, then it should, where tax crimes are predicate offences to money laundering, file appropriate suspicious activity reports.

10. Employees

Private banks may find that some of their money laundering risks are actually quite close to home. These include insider dealing by client advisers, through relationships with customers who may be themselves "Insiders", or as a result of working in a universal bank with an investment bank and getting unauthorised access to information or being tipped off or through other outside contacts; for misuse or interaction through front and/or parallel trading in connection with large customer orders. Also a client adviser may exceed his authority with respect to customer activity and/or divert customer assets for their own benefit whether to make personal gain or to cover earlier undisclosed losses.



Sub-section 4. Country Risks

- Country Risks Methodology & Sources, 215
- Financial Action Task Force/FATF, 215
- Sanctioned Countries, 216
- Wolfsberg Group, 217
- Basel Institute of Governance, 218
- Additional Country Sources, 218
- Hot Spots (in-country and Regional), 221
- Diversion Risk or Close Proximity Risk, 221
- Free Trade Zones, 222
- Time Zone Risk, 222

Country Risks

Methodology & Sources

One of the most important money laundering risk factors to be considered is country risk, particularly with respect to a customer's exposure to a particular country where money laundering risk is considered problematic, material or increased. Whilst there is no universally accepted list of increased risk countries from a money laundering or financing of terrorism perspective and moreover where there is no accepted methodology, there are growing commonalities in modalities and similarities in outcomes amongst many financial institutions. First the FATF has listed some countries as recently as February 2013 as presenting increased risks. Additionally a number of these countries as well as some others are subject to various forms and levels of sanctions and embargoes from the UN or national governments and many others are the subject of numerous ratings that can be useful to evaluate respective and relative risks.

Nevertheless, whilst useful, these country commentaries apply to a limited number of countries. Fortunately there are a number of sources that can be used to cover many, if not most countries in the world, though in each case they are focussed on a particular area, for example, corruption or drug trafficking, and so combining these sources may make the most sense. In addition to particular financial crime risks, it is widely believed that the political and economic stability of a country, its record on Human Rights and on the Rule of Law are good proxies to base any financial crime country risk model on.

At UBS we have long since developed and continue to improve a methodology which incorporates many of the direct money laundering and indirect political and economic risks into a comprehensive Country Risk Methodology but this is not the only model, in fact many financial institutions have their own model. The Basel Institute on Governance recently published its own thoughts on country risk which is also available for financial institutions to use.

The following sections contain more specific information from FATF, identifies countries that are subject to sanctions and embargoes, and other credible and useful sources of information for use in assessing country risk.

Financial Action Task Force

High-Risk and Non-Cooperative Jurisdictions

The principal and initial objective of the FATF Non-Cooperative Countries and Territories ("NCCT") initia-

tive was to reduce the vulnerability of the financial system to money laundering by ensuring that all financial centres adopt and implement measures for the prevention, detection and punishment of money laundering according to internationally recognised standards. The FATF initially designated countries as "non-co-operative in the global fight against money laundering", named NCCTs. The FATF recommended that financial institutions give special attention to transactions involving the NCCTs, in accordance with the former Recommendation 21.

In February 2000, the FATF defined the basic procedure for reviewing countries and territories as well as 25 NCCT criteria against which relevant laws, regulations and other relevant information were analysed. In 2000 and 2001 47 countries or territories were examined of which 15 were listed as NCCTs in 2000 (Bahamas, Cayman Islands, Cook Islands, Dominica, Israel, Lebanon, Liechtenstein, Marshall Islands, Nauru, Niue, Panama, Philippines, Russia, St. Kitts and Nevis, St. Vincent and the Grenadines) and subsequently 8 in 2001 (Egypt, Grenada, Guatemala, Hungary, Indonesia, Myanmar, Nigeria, and Ukraine). The FATF did not review any new jurisdictions since 2001 in the framework of the NCCT initiative. As of October 2006, there have been no NCCTs in the context of the NCCT initiative with Myanmar being the country which was removed last from the NCCT list.

In order to protect the international financial system from money laundering and financing of terrorism risks and to encourage greater compliance with these FATF recommendations, the FATF identified jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international finance system.

Following the FATF International Co-Operation Review Group (ICRG) review, jurisdictions are publicly identified in one of two FATF public documents that are issued three times a year. The first public document, named "FATF's Public Statement", the most recent being issued in February 2013, identifies (i) jurisdictions that have strategic anti-money laundering and (ii) counter financing of terrorism deficiencies and to which counter-measures apply and jurisdictions with strategic anti-money laundering and counter financing of terrorism deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies. The second FATF public document, also issued in February 2013 named "Improving Global AML/CFT Compliance: On-going Process" identifies jurisdictions with strategic anti-money laundering and

counter financing of terrorism deficiencies that have provided a high-level political commitment to address the deficiencies through implementation of an action plan developed with the FATF.

Public Statement February 2013¹

FATF continues to publicly name and shame two countries as presenting the most risks and calls on its members and other jurisdictions to apply counter-measures to protect the international financial system from the on-going and substantial money laundering and terrorist financing risks emanating from these jurisdictions.

Countries Where Counter Measures are Required

Iran	North Korea
------	-------------

Source: FATF (as of February 2013)

In the next worst category FATF in February 2013 has named and shamed a further 13 countries as having strategic AML/CFT deficiencies but stopped short of calling for outright counter-measures.

FATF announced that Bolivia, Cuba, Sri Lanka and Thailand have each provided FATF with commitments and action plans and have been moved to the next level status below. FATF accepted Turkey had made improvements and agreed it was not necessary to suspend Turkey's membership. Still Turkey stays on this former list.

Countries with Strategic AML/CFT Deficiencies

Ecuador	São Tomé & Príncipe
Ethiopia	Syria
Indonesia	Tanzania
Kenya	Turkey*
Myanmar	Vietnam
Nigeria	Yemen
Pakistan	

Source: FATF (as of February 2013)

Public Statement February 2013

FATF also published a third list of 24 countries in February 2013 which whilst strategic deficiencies exist have committed to fix these. Of these, Morocco and Tajikistan are highlighted as both making insufficient progress and as such being placed on the watch for a downgrade. Due to their progress, both Ghana and Venezuela are removed from the list.

Jurisdictions - with Weaknesses but Agreed Action Plans

Afghanistan	Mongolia
Albania	Morocco
Algeria	Namibia
Angola	Nepal
Antigua & Barbuda	Nicaragua
Argentina	Philippines
Bangladesh	Sri Lanka
Brunei Darussalam	Sudan
Cambodia	Tajikistan
Cuba	Thailand
Kuwait	Zimbabwe
Kyrgyzstan	

Source: FATF (as of February 2013)

See also Breaking News below at the end of this Book.

Sanctioned Countries

Whilst the imposition of sanctions and embargoes has long been used as a political tool, its use appears to be on the increase with over 30 countries subject to some form of formal sanction either from the UN, US, EU, Switzerland, Australia, New Zealand, the Arab League or Israel. The most important are as follows:

United Nations

Under Chapter VII of the Charter, the UN² can take enforcement measures to maintain or restore international peace and security. Such measures range from economic and/or other sanctions not involving the use of armed force to international military action. The range of sanctions has included comprehensive economic and trade sanctions and/or more targeted measures such as arms embargoes, travel bans, financial or diplomatic restrictions. Sanctions resolutions have been enforced against Somalia and Eritrea, concerning Al-Qaeda and associated individuals and entities, Liberia, the Democratic Republic of Congo, Iraq and Kuwait (senior officials of the former Iraqi regime and their immediate family members, including entities owned or controlled by them or by persons acting on their behalf), Côte D'Ivoire, Sudan, concerning the terrorist bombing in Beirut, Lebanon that killed former Lebanese Prime Minister Rafiq Hariri and 22 others, Democratic People's Republic of Korea, Islamic Republic of Iran, Libya, concerning any individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, and Guinea-Bissau.

European Union (EU)

Within the framework of the Common Foreign and Security Policy (CFSP), the EU applies restrictive measures in pursuit of the specific CFSP objectives set out in Article 11 of the Treaty on European Union.³

Sanctions or restrictive measures have been frequently imposed by the EU in recent years, either on an autonomous EU basis or implementing binding resolutions of the Security Council of the UN.

Sanctions are an instrument of a diplomatic or economic nature which seek to bring about a change in activities or policies such as violations of international law or human rights, or policies that do not respect the rule of law or democratic principles.

Restrictive measures in force include:⁴ Afghanistan, Al-Qaeda and other terrorist groups (foreign terrorist organisations), Belarus, Bosnia and Herzegovina, Burma, China, Democratic Republic of Congo, Côte D'Ivoire, Egypt, Eritrea, Republic of Guinea (Conakry), Guinea-Bissau, Haiti, Iran, Iraq, Democratic People's Republic of Korea (North Korea), Lebanon, Liberia, Libya, Moldova, Myanmar (Burma), Serbia and Montenegro, Somalia, South Sudan, Sudan, Syria, Tunisia, US and Zimbabwe.

US/OFAC

The Office of Foreign Assets Control (OFAC) administers a number of different financial country-specific (and non-country specific) sanctions programmes. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals. Current programmes include Balkans, Belarus, Burma, Ivory Coast, Counter Narcotics Trafficking, Counter Terrorism, Cuba, Democratic Republic of Congo, Iran, Iraq, Lebanon, former Liberian Regime of Charles Taylor, Libya, Non-Proliferation, North Korea, Rough Diamond Trade Controls, Somalia, Sudan, Syria, transnational criminal organisations, Yemen, and Zimbabwe.

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programmes that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" (SDNs). Their assets are blocked and US persons are generally prohibited from dealing with them.

Switzerland/SECO

Within the framework of the Swiss Sanctions and Embargo law (Article 1) Switzerland applies restrictive measures in adherence to public international law, in particular observation of human rights, in alignment with the UN, the Organisation for Security and Cooperation in Europe (OSCE), or the most important

trade partners of Switzerland. Current measures⁵ apply mostly to persons in Iraq, former Republic of Yugoslavia, Liberia, Myanmar, Zimbabwe, Côte D'Ivoire, Sudan, Democratic Republic of Congo, terrorist bombing in Beirut, Lebanon that killed former Lebanese Prime Minister Rafiq Hariri and 22 others, Belarus, Democratic People's Republic of Korea (North Korea), Lebanon, Iran, Somalia, Guinea, Eritrea, Libya, Syria, and Guinea-Bissau.

Others

There are a number of additional notable sanctions issued by important parties, including by the OSCE that have designated Armenia, by Australia and New Zealand who have designated Fiji, by the Arab League against Israel and by Israel against the Palestinian territories.

For more detailed information on Sanctions and Embargoes including details about Country Programmes see Part 1, Section 3, Sanctions & Embargoes below.

Wolfsberg Group

Within its aim to develop financial services industry standards, and related products, for KYC, anti-money laundering and counter terrorist financing policies, the Wolfsberg Group dedicated itself to country risk on numerous occasions. In 2006, the Wolfsberg Group published guidance on a Risk Based Approach for Managing Money Laundering Risks⁶ where Country Risk was one of the risk criteria, which may be modified by risk variables, to measure money laundering risks. As referenced in this Wolfsberg statement: *"Country risk [...] provides useful information as to potential money laundering risks. There is no universally agreed definition by either government or institutions that prescribes whether a particular country represents a higher risk. Factors that may result in a determination that a country poses a higher risk include:*

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the UN. In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognised, may be given credence by an institution because of the standing of the issuer and the nature of the measures.

- Countries identified by FATF as non-cooperative in the fight against money laundering or identified by credible sources as lacking appropriate money laundering laws and regulations.

- Countries identified by credible sources as providing funding or support for terrorist activities. (while, as stated below, a risk based approach to identifying terrorist funding in financial institutions is impracticable, considering those countries that support terrorist activities as an

evaluating factor for determining country or geography risk may be appropriate.)

- Countries identified by credible sources as having significant level of corruption, or other criminal activities."

Basel Institute of Governance

The Basel AML Index⁷ is an example of a country risk ranking from the Basel Institute of Governance which measures the risk of serious crimes such as money laundering and financing of terrorism as well as other relevant aspects such as financial standards and public transparency.

The Basel AML Index is offered in a public and an expert edition. The public edition is free and accessible online. The expert edition includes extensive additional functionalities (for example, an overall score with sub-indicators and sanctions lists, more comprehensive list with particular country ratings, a data file download option, updates at regular intervals upon data availability and provision of expert advice and tailor-made solutions) is available for an annual fee.

The Basel AML Index uses a composite methodology sourced through publicly available third party data.

The data aggregated in the index to assess a country's overall risk consists of a composition of fifteen variables dealing with relevant regulations combating money laundering and countering terrorist finance, financial standards, transparency and disclosure, and political risks.

The overall risk of a country is expressed in a score which is based on the 15 variables and a weighting scheme pre-defined through a qualitative expert assessment.

The 15 variables or indicators are grouped in the following five categories. Each of the indicators which have been normalized into a zero (low risk) to ten (high risk) scale and categories (indicated in parentheses below) have their own weighting:

Basel AML Index - Sources and Weightings	
Money Laundering / Terrorist Financing Risk (65%)	<ul style="list-style-type: none"> – FATF Recommendations on Money Laundering and Terrorist Financing – Tax Justice Network (TJN) – Financial Secrecy Index – US International Narcotics Control Strategy Report (INCSR) Volume II on Money Laundering
Corruption Risk (10%)	<ul style="list-style-type: none"> – Transparency International Corruption Perceptions Index (TI CPI)
Financial Transparency and Standards (15%)	<ul style="list-style-type: none"> – World Bank Doing Business Ranking – Business Extent of Disclosure Index – World Economic Forum – Global Competitiveness Report (WEF GCR) – Strength of Auditing and Reporting (scores selected from the Executive Opinion Survey) – World Economic Forum – Global Competitiveness Report (WEF GCR) – Regulations of Securities (scores selected from the Executive Opinion Survey) – World Bank – IDA Resource Allocation Index (IRAI) – Financial Sector (category selected)
Public Transparency and Accountability (5%)	<ul style="list-style-type: none"> – International IDEA Political Finance Database – International Budget Partnership (IBP) - Open Budget Index – World Bank – IDA Resource Allocation Index (IRAI) – Transparency, Accounting and Corruption (category selected)
Political and Legal Risk (5%)	<ul style="list-style-type: none"> – Euromoney – Political Risk – Freedom House – Freedom in the World & Press Freedom Index – World Economic Forum – Global Competitiveness Report (WEF GCR) – Institutional Strength (scores selected from the Executive Opinion Survey) – Bertelsmann Stiftung Transformation Index (BTI) – Rule of Law scores

Source: Basel Institute of Governance

Additional Country Sources

Beyond FATF UBS own methodology and that of the Basel Institute on Governance ("BIG") the following (some of which are included in the UBS and/or BIG methodologies) are interesting resources for country risk assessments.

Bertelsmann Stiftung's Transformation Index (BTI)⁸

The Bertelsmann Stiftung's Transformation Index (BTI) analyses and evaluates the quality of democracy, market economy and political management in 128 developing and transition countries. It measures successes and setbacks on the path toward a democracy based on the rule of law and a market economy flanked by socio-political safeguards. Within this framework, the BTI publishes two rankings, the Status Index and the Management Index.

In-depth country reports provide the qualitative data used to assess these countries' transformation status and challenges, and to evaluate the ability of policymakers to carry out consistent and targeted reforms. The BTI is the first cross-national comparative index that uses self-collected data to measure the quality of governance and provide a comprehensive analysis of countries' policymaking success during processes of transition.

The Status Index ranks the countries according to their state of democracy and market economy as of spring 2011. The Management Index ranks the countries according to their leadership's political management performance between 2009 and 2011.

Control Risks – Risk Module including Political Operational, Security, and Terrorism Rating⁹

Control risks provide a number of risk ratings that can be considered useful including:

Political Rating - Political risk evaluates the likelihood of state or non-state political actors negatively affecting business operations in a country through regime instability or direct/indirect interference.

Operational Rating - Operational risk evaluates the influence of societal and structural factors on business activity in a country, and the likelihood of state and non-state actors either facilitating or impeding efficient business operations.

Security Rating - Security risk evaluates the likelihood of state or non-state actors engaging in actions that harm the financial, physical and human assets of a company, and the extent to which the state is willing and able to protect those assets.

Terrorism Rating - Terrorism risk evaluates the likelihood that acts of terrorism directly or indirectly affect business operations in a country.

Egmont Group¹⁰

The Egmont Group is an association of governmental Financial Intelligence Units (FIUs) who meet regularly to find ways to co-operate especially in the areas of information exchange, training and the sharing of expertise in relation to money laundering and the financing of terrorism. It is named after the Egmont Arenberg Palace in Brussels where a first meeting of

FIUs was held in 1995. Membership is open to national FIUs but is subject to conditions and compliance with set criteria. Membership of Egmont should be seen as a positive signal towards a member country.

Euromoney Country Risk Rating¹¹

Euromoney's Country Risk Rating evaluates the investment risk of a country, such as risk of default on a bond, risk of losing direct investment, risk of global business relations etc., by taking a qualitative model, which seeks an expert opinion on risk variables within a country (70% weighting) and combining it with three basic quantitative values (30% weighting). Factors included in the ranking of countries by risk: political risk, economic performance/projections, structural assessment, debt indicators, credit ratings, access to bank finance, and access to capital markets. The Euromoney Political Risk Rating measures the risk of non-payment or non-servicing of payment for goods or services, loans, trade-related finance and dividends, and the non-repatriation of capital.

EU - Common Understanding of the Procedure on Criteria for the Recognition of Third Countries' Equivalence agreed by Member States¹²

Third countries meeting EU anti-money laundering and counter financing of terrorism equivalence standards are regularly identified in order to apply some of the EU's 3rd AML Directive's provisions on, for example, simplified due diligence. In the context of this obligation and in order to coordinate their approach on equivalence, member states have agreed a list of equivalent third countries. The list, which is regularly assessed includes currently: Australia, Brazil, Canada, Hong Kong, India, Japan, South Korea, Mexico, Singapore, Switzerland, South Africa, and the US though to be effective member states should also adopt the list which, for example, France, Italy and Germany have done, UK effectively also, whilst Luxembourg has but requires more and Ireland has but also adds extra states too. It should be noted that future EU proposals (EU draft 4th Money Laundering Directive) will no longer use equivalent lists for third countries, though EU countries only will be assured equivalent. Beyond the EU, other states currently identify other so-called "Equivalent Countries", for example, Hong Kong deems all FATF members as "equivalent"; A number of offshore centres like Jersey, Guernsey, Isle of Man and the Cayman Islands have also adopted the EU list as well as each other (to be verified). States that have adopted no list or identified any countries include Australia, Japan, Singapore, Switzerland, and the US.

Freedom House - Freedom in the World¹³

Freedom in the World, Freedom House's flagship publication, is the standard setting comparative assessment of global political rights and civil liberties. Published annually since 1972, the survey ratings and narrative reports on 195 countries and 14 related and disputed territories are used by policymakers, the media, international corporations, civic activists, and human

rights defenders to monitor trends in democracy and track improvements and setbacks in freedom worldwide. The Freedom in the World data and reports are available in their entirety on the Freedom House website.

OECD: International Tax Standards¹⁴

The Global Forum on Transparency and Exchange of Information for Tax Purposes met in 2011 and adopted a report delivered to the G20 on the progress it has made in ensuring the implementation of the international standard in tax cooperation. A progress report of 18 May 2012 indicated that all jurisdictions surveyed by the Global Forum had fully committed to the most recent internationally agreed tax standard. Two countries, Nauru and Guatemala, had in principle committed themselves to the internationally agreed tax standard, but had not yet substantially implemented it.

Transparency International Corruption Perceptions Index¹⁵

First launched in 1995, the Corruption Perceptions Index ("CPI") has been widely credited with putting the issue of corruption on the international policy agenda. It measures the perceived levels of public sector corruption in 183 countries and territories. The CPI ranks countries/territories based on how corrupt their public sector is perceived to be. It is a composite index, a combination of polls, drawing on corruption-related data collected by a variety of reputable institutions. The CPI reflects the views of observers from around the world, including experts living and working in the countries or territories evaluated.

Transparency International – Global Corruption Barometer¹⁶

The Global Corruption Barometer is the only world-wide public opinion survey on corruption. TI's Barometer is the largest cross-country survey to collect the general public's views on, and experiences of, corruption. In 2010 and 2011 the Barometer interviewed more than 100,000 people in 100 countries, making it the most comprehensive round since the survey was launched in 2003. The Barometer explores the general public's views about corruption levels in their country as well as their governments' efforts to fight corruption. The 2010/11 Barometer also probes the frequency of bribery, reasons for paying a bribe in the past year, and attitudes towards reporting incidents of corruption.

US Department of State Country Report of Terrorism - supporters of International Terrorism (Bureau of Counter Terrorism)¹⁷

The Country Report on Terrorism 2011 provides the Department of State's annual, statutorily mandated assessment of trends and events in international terrorism that transpired, including country-by-country breakdowns of foreign government counterterrorism co-operation, and profiles of designated terrorist organisations. As well as identifying countries experiencing terror activities it identifies State Sponsors of Terrorism which are Cuba, Iran, Sudan and Syria.

US Department of State – International Narcotics Control Strategy Report (INCSR)¹⁸

The Department of State's International Narcotics Control Strategy Report (INCSR) is the US Government's annual country-by-country two volume report that describes the efforts to attack all aspects of the international drug trade, chemical control, money laundering and financial crimes. Volume I covers drug and chemical control activities. Volume II covers money laundering and financial crimes.

US State Department - Trafficking in Persons Report 2010 (TIP) including Human Trafficking Tier Lists¹⁹

The Department of State prepared this report using information from US embassies, government officials, NGOs and international organisations, published reports and research trips. US diplomatic posts and domestic agencies reported on the trafficking situation and governmental action based on research that included meetings with a wide variety of government officials, local and international NGO representatives, officials of international organisations, journalists, academics, and survivors. Every US mission overseas employs at least one officer covering human trafficking issues. The US State Department places each country into one of three tiers. This placement is based more on the extent of government action to combat trafficking than on the size of the problem, although the latter is also an important factor. The analyses are based on the extent of governments' efforts to reach compliance with the TVPA's minimum standards for the elimination of human trafficking.

Fund for Peace (FFP) - The Failed States Index (2012) – The US think-tank²⁰

The Fund for Peace (FFP) is an independent, nonpartisan, non-profit research and educational organisation working to prevent violent conflict and promote sustainable security. FFP promotes sustainable security through research, training and education, engagement of civil society, building bridges across diverse sectors, and developing innovative technologies and tools for policy makers. FFP focuses on the problems of weak and failing states. Each year FFP releases its Failed States Index, a country ranking based on a set of indicators assessing stability and vulnerability. FFP hopes that governments and NGOs can use it as a policy tool for improvements.

The World Bank Group - Worldwide Governance Indicators (WGI)²¹

The Worldwide Governance Indicators (WGI) project reports aggregate and individual governance indicators for 213 economies over the period 1996–2010, for six dimensions of governance: Voice and Accountability, Political Stability and Absence of Violence, Government Effectiveness, Regulatory Quality, Rule of Law, and Control of Corruption. The aggregate indicators combine the views of a large number of enterprise, citizen and expert survey respondents in industrial

and developing countries. The individual data sources underlying the aggregate indicators are drawn from a diverse variety of survey institutes, think tanks, non-governmental organisations, and international organisations.

The World Bank Group - Ease of Doing Business Index 2012²²

Economies are ranked on their ease of doing business, from 1 – 183. A high ranking on the ease of doing business index means the regulatory environment is more conducive to the starting and operation of a local firm. This index averages the country's percentile rankings on 10 topics, made up of a variety of indicators, giving equal weight to each topic. The rankings for all economies are benchmarked to June 2011.

Doing Business 2012 is the ninth in a series of annual reports investigating the regulations that enhance business activity and those that constrain it. Doing Business presents quantitative indicators on business regulation and the protection of property rights that can be compared across 183 economies from Afghanistan to Zimbabwe and over time. The 2012 report presents results for two aggregate measures: the aggregate ranking on the ease of doing business and a new measure, the "distance to frontier." While the ease of doing business ranking compares economies with one another at a point in time, the distance to frontier measure shows how much the regulatory environment for local entrepreneurs in each economy has changed over time.

Further Resources

The following website has a lot of useful information and could be a helpful resource.

KnowYourCountry.com²³

The aim of KnowYourCountry.com is to gather relevant information and data from legitimate sources, collate it, and provide it to the public in a concise and manageable form, which is helpful in consideration of a particular country risk in the course of conducting business.

Hot Spots (in-Country and Regional)

Whilst most Country Risk Models provide a score and/or a rating on the Country level, the most sophisticated models also take into consideration other factors, for example, sub-country ratings, in particular for areas of countries where the risk is significantly different or areas that span parts of a number of countries. For example, in the US a number of in-country regions are well known and identified as High Intensity Drug Trafficking Area/High Intensity Financial Crime Area, including areas such as New York and New Jersey, areas of Chicago and Los Angeles and around Northern and Southern California, the South West border area, South Florida and Puerto Rico. Elsewhere in the world

in-country hot spots or regional hot spots can be identified which could increase the risk beyond the general country risk rating where exposure is to these areas. For more details see Part 2, Section 5, Regions, Countries, Criminals & Terrorists.

Hot Spots (in-Country & Regional)

Americas	
US	
- HIDTA/HIFCA	
Latam	
- Tri-border Area	
Asia	
- Eastern Asia	
- China Xinjiang/East Turkistan	
- Tibet	
- Macau	
- Southern Asia	
- Kashmir & Jammu	
- NE India/Seven Sisters	
- Sri Lanka/Jaffna Peninsula	
- Af/Pak - Kandahar, SWAT Valley, Balochistan, Federally Administered Tribal Areas	
- South-East Asia	
- Southern Philippines/Southern Thailand (Islamic Regions)	
- Golden Triangle	
Middle East	
- Palestinian Territories - Gaza Strip	
- Lebanon - Bekaa Valley	
- Turkey/Iraq - Kurdistan	
- Dubai and Sharjah, UAE	
Europe	
- Western Europe	
- Northern Ireland/UK	
- Basque Country/Spain & France	
- Corsica, France	
- Italy-Sicily, Naples, Puglia, Calabria	
- Holy See, Vatican	
- Eastern Europe	
- Chechnya & Ichkeria	
- Crimea, Ukraine	

Source: see Part 2, Section 5, Regions, Countries, Criminals and Terrorists below

Diversion Risk or Close Proximity Risk Countries

Other areas where country risk may be important are those countries that could be seen as either in close geographical proximity to and/or have close commercial ties with sanctioned countries, with, for example, close commercial ties based on imports and exports as a percentage (%) of the commercial ties' country's Gross Domestic Product ("GDP").

The following is an example list.

Diversion Risk or Close Proximity Countries	
Afghanistan	Kuwait
Armenia	Kyrgyzstan
Azerbaijan	Lebanon
Central African Republic	Macau
Chad	Pakistan
Cyprus	Somalia
Egypt	Tajikistan
Eritrea	Turkey
Ethiopia	Turkmenistan
Iraq	Uganda
Jordan	United Arab Emirates
Kazakhstan	Uzbekistan
Kenya	Yemen

Free Trade Zones

Free Trade Zones (FTZs) have proliferated in recent years with conditions that make FTZs attractive to legitimate business also attract abuse by illicit actors, and according to the Financial Action Task Force (FATF) are a continuing concern.²⁴

According to a FATF report issued in 2011²⁵ there are approximately 3,000 FTZs in 135 countries around the world with a total turnover in the billions of US\$. FTZs are designated areas within jurisdictions in which incentives are offered to support the development of exports, foreign direct investment (FDI), and local employment. These incentives include exemptions from duty and taxes, simplified administrative procedures and the duty free importation of raw materials, machinery, parts and equipment. In addition to boosting economic opportunity, illicit actors have been able to launder the proceeds of crime, conducting unusual business activity, with concerns over trade-based money laundering (TBML), finance terrorism and facilitating WMD proliferation. In particular critics claim the lack of oversight by competent domestic authorities and weak procedures to inspect goods and register legal entities, including inadequate record-keeping and information technology systems and a lack of adequate co-ordination and co-operation between zone and Customs authorities encourages criminal activity. The misuse of free trade zones impacts all jurisdictions including those without FTZs of their own, because goods can originate from or be transshipped through FTZs not subject to adequate export controls. Proliferators of weapons of mass

destruction (WMD) abuse FTZs to tranship dual use goods and to disguise the final destination of sensitive items. FTZs can also be used to create legal entities and access the international financial system, providing opportunities to launder illicit proceeds. Many major zones are also located in regional financial centres linking international trade hubs with access to global centres of finance.

According to the BASCAP report, "Controlling the Zone: Balancing facilitation and control to combat illicit trade in the world's Free Trade Zones",²⁶ FTZs are particularly vulnerable to counterfeiting and piracy, due to lax enforcement of intellectual property rights.

Top Free Zones of the Future - 2012/13 Overall		
1. Dubai Airport FZ	UAE	
2. Dubai Airport IFC	UAE	
3. Shanghai Waigaoqiao FTZ	China	
4. Iskander	Malaysia	
5. Dubiotech	UAE	
6. Tangier FZ	Morocco	
7. Freeport of Ventspils	Latvia	
8. The Clark Freeport Zone	Philippines	
9. Chittagong Export Process Zone	Bangladesh	
10. Dubai Media City	UAE	

Source: FDI Magazine June/July 2012²⁷

Time Zone Risk

Whilst not per se, an obvious area to identify Country Risk aspects, the difference between, for example, a customer's home domicile to other attributes of risk whether client risk factors such as the use of Panama Foundations for a French customer, or the opening of bank accounts in Singapore for a Canadian or the wiring of funds via China for a Brazilian may be an important risk indicator. Using distance by utilising time to judge Country exposure may produce interesting results.



Section 3

Money Laundering Laws & Regulations

- Introduction, 225
- AML Treaties, Conventions & Major Laws, 226
- Financial Action Task Force/FATF, 245
- Wolfsberg Group AML Standards & Work, 259
- Sanctions & Embargoes, 264

Introduction

To try to address the transnational threat posed by criminals bent on committing serious crimes and terrorists aiming at creating mayhem, governments have long worked together to fashion common agreements to respond to these threats. Many treaties and conventions have been adopted with a recognition that such instruments are necessary to harmonise approaches and to foster international cooperation. Whilst many International Instruments have been adopted over the last 30 years, the history of using international legal instruments to address collective concerns and to counter serious transnational criminality, is a much longer one. Since the beginning of the 20th century, efforts have been made to put in place an international drug control framework and to continually build on agreements reached. This process started with the 1909 Opium Conference in Shanghai¹ and to the landmark convention in 1912 in the Hague (the Netherlands) with the signing of the International Opium Convention² which the major powers committed to and led to the start of the criminalisation of the supply of opium.

Landmark ML Related Instruments	
1	1912 - The Hague Convention
2	1933 - US Securities Act
3	1934 Securities & Exchanges Act
4	1970 - Organised Crime Control Act/Bank Secrecy Act
5	1977 - Swiss Bankers Association Code on due diligence
6	1977 - US Foreign Corrupt Practices Act
7	1986 - US ML Control Act
8	1988 - Vienna Convention
9	1990 - FATF 40 Recommendations
10	1998 - BCBS Prevention of criminal use of the banking system for the purpose of ML
11	2000 - The Palermo Convention
12	2001 - US Patriot Act
13	2001 - FATF 8 Sp Recs on TF
14	2003 - UN Convention against Corruption
15	2005 - EU Market Abuse Directive

Source: Author

drugs followed, as did chemical biological and nuclear weapons treaties, aircraft safety responding to terrorist threats and events and organised crime, anti-corruption, terrorism and WMD proliferation treaties, human trafficking and environmental protection amongst the most important. Many of these followed individual leadership by countries, particularly the US, where organised crime, anti-corruption and anti-money laundering instruments were first introduced.

Whilst treaties and conventions have played a major role in securing broad agreement and co-operation, it was recognised that an inter-governmental body was required to tackle money laundering and in 1989 at the behest of the G7 FATF was born, and a year later in 1990 FATF promulgated its first 40 Recommendations which were then revised and supplemented on numerous occasions, the most recent in 2012 where the 9 Special Recommendations on combating terrorism finance have been amalgamated with the 40 Recommendations on money laundering. These most recent standards come just over 100 years since the Hague International Drugs Convention and were implemented in 2013 and 2014, 25 years after the establishment of FATF.

As far as the financial institutions are concerned, and beyond public standard setters the Wolfsberg Group issues statements and provide standards for financial institutions to consider.

In this Part 1, Section 3 a chronology of the most important treaties and conventions, a number of the most important laws that have had international impact in the AML, Bribery and Corruption and Terror Finance field are set out, followed by a summary of FATF's work and an extract of the 2012 40 Recommendations, as well as a summary of the statements and work carried out by the Wolfsberg Group. Finally a summary of leading Sanctions and Embargoes Laws, complete this Section 3.

AML Treaties, Conventions & Major Laws



1912 - The International Opium Convention (the "Hague Convention")¹

The US convened a 13-nation conference of the International Opium Commission in 1909 in Shanghai, China in response to increasing criticism of the opium trade. The treaty was signed by Germany, the US, China, France, the UK, Italy, Japan, the Netherlands, Persia, Portugal, Russia, and Siam. The Convention provided that "The contracting powers shall use their best endeavours to control, or to cause to be controlled, all persons manufacturing, importing, selling, distributing, and exporting morphine, cocaine, and their respective salts, as well as the buildings in which these persons carry such an industry or trade. The Convention went into force globally in 1919 when it was incorporated into the Treaty of Versailles.

1925 - The International Opium Convention (the "Geneva Convention")²

This Convention introduced a statistical control system to be supervised by a Permanent Central Opium Board. Egypt, with support from China and the US, recommended that a prohibition on hashish be added to the Convention.

1925 - The Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare (the "Geneva Protocol")³

This Treaty prohibited the first use of chemical and biological weapons. It prohibited the use of chemical weapons and biological weapons, but had nothing to say about production, storage or transfer. Later treaties covered these aspects (see the 1972 Biological Weapons Convention and the 1993 Chemical Weapons Convention).

1933 - The USA Securities Act⁴

The Securities Act of 1933 was "enacted as a result of the market crash of 1929. The Securities Act of 1933 is also known as the "Truth in Securities Act". The 1933 Act was based on the idea that companies offering securities should provide potential investors with sufficient information about both the issuer and the securities to make an informed investment decision. The legislation had two main goals: (1) to ensure more transparency in financial statements so investors can make informed decisions about investments, and (2) to

establish laws against misrepresentation and fraudulent activities in the securities markets. The Securities Act of 1933 was the first major piece of federal legislation regarding the sale of securities. Prior to this legislation, the sale of securities was primarily governed by state laws; however, the market crash of 1929 raised some serious questions about the effectiveness of how the markets were being governed. Due to the turmoil surrounding the investing community at this time, the federal government had to bring back stability and investor confidence in the overall system.

1933 - USA Banking Act (Glass-Steagall Act)⁵

In 1933 in the aftermath of the Great Depression and widespread bank failures, Congress enacted the Banking Act of 1933. Four sections of the Act are referred to as the Glass-Steagall Act. Many critics believed that banks had engaged in inappropriate securities activities that harmed investors. The Glass-Steagall Act addressed these concerns in a very broad way: Section 16 restricted commercial national banks from engaging in investment banking; Section 20 prohibited any member bank from affiliating in specific ways with an investment bank; Section 21 restricted investment banks from engaging in any commercial banking; and Section 32 prohibited investment bank directors, officers, employees or principals from serving in those capacities at a commercial member bank of the Federal Reserve System. Some believe President Franklin D. Roosevelt signed the 1933 Glass-Steagall Act, specifically targeted at and breaking up JP Morgan & Co.

1934 - USA Securities & Exchange Act⁶

The Securities Exchange Act of 1934, also called the Exchange Act, '34 Act, or Act of '34, is a law governing the secondary trading of securities (stocks and bonds) in the US. The Act and related statutes form the basis of regulation of the financial markets and their participants in the US. The 1934 Act also established the Securities and Exchange Commission (SEC), the agency primarily responsible for enforcement of US federal securities law. The Act regulates the secondary trading of securities that companies issue in the primary market, between persons often unrelated to the issuer, frequently through brokers or dealers. One area subject to the Act is the actual securities exchange, the place where many people purchase and sell US securities (stocks and bonds). The Act also regulates broker-dealers. The 1934 Act addressed insider trading directly and has been supplemented by later SEC rulemaking and case law.

1936 - The USA Commodity Exchange Act⁷

The Commodity Exchange Act became the Grain Futures Act and extended Federal regulation to a list of commodities that included cotton, rice, mill feeds, butter, eggs, and Irish potatoes, as well as grains. The Grain Futures Commission became the Commodity Exchange Authority and would later become the Commodity Futures Trading Commission (CFTC) and is responsible for regulating US Futures and Options Markets.

1942 - USA Exchange Act Rule 10b-5⁸

In 1942, the SEC was presented with a situation in which the president of a company was buying shares from the existing shareholders at a low price by misrepresenting the company's financial condition. While Securities Act S17(a) (1) prohibited fraud and misstatements in the sale of securities, there was no comparable provision prohibiting such practices in connection with the purchase of securities. The SEC's Assistant Solicitor accordingly lifted the operative language out of S17(a), made the necessary modifications, added the words 'in connection with the purchase or sale of any security,' and presented the product to the Commission as Securities Exchange Act Rule 10b-5. It was unanimously approved without discussion. In the more than 50 years since its adoption, this simple rule has been involved in countless SEC and private proceedings, and applied to almost every conceivable kind of situation. In the 1960s and early 1970s, many federal appellate courts and district courts developed expansive interpretations of Rule 10b-5 (and other antifraud provisions of the securities laws).

1961 - Single Convention on Narcotic Drugs (amended by 1972 Protocol)⁹

The 1961 Single Convention was intended to codify most of the numerous international drug conventions dating back to 1912, and placed under international control primarily plant-based substances such as coca, marijuana and opium, as well as their derivatives. Acknowledging the need for medicinal opiates, states parties were obliged to submit estimates to an independent committee (the International Narcotics Control Board) of their opiate needs for the coming year. A 'statistical returns system' was also created in the 1961 Single Convention to assess state implementation of its terms. It included information relating to the production of drugs, drug consumption and imports/ exports of controlled substances. The 1972 Protocol to the 1961 Single Convention expanded the role of the International Narcotics Control Board in relation to the illicit production, use and traffic in narcotic drugs.

1969 – Convention on Offences and Certain Other Acts Committed On Board Aircraft (the “Tokyo Convention”)¹⁰

This international treaty was signed in Tokyo on 14 September 1963 and entered into force on 4 December 1969. The Convention created offences for any acts jeopardising the safety of persons or property on board civilian aircraft while in-flight and engaged in international air navigation. Coverage included the commission of or the intention to commit offences and certain other acts on board an aircraft.

1970 - USA/Organised Crime Control Act¹¹

The Organised Crime Control Act was the US legislative response to combat organised crime. The legislation followed Congressional hearings in the late 1950s into the early 1960s that identified to the public

the breadth and pervasiveness of organised crime in the US, including its control over international labour unions, and other important areas of US business and trade. A critical component of this provision was the passage of the Racketeer Influenced and Corrupt Organisations Act¹² (RICO Act). This provision was designed to provide an important prosecutorial tool to allow law enforcement to attack corruption on an "enterprise" basis. Although, it was primarily intended to attack organised crime families, its use has been expanded to non-organised crime organisations, such as security fraud cases. The statute allows prosecutors to charge different members of the organisation under one scheme, with significant criminal sanctions, whether it be the leader who directed the criminal scheme or the actors themselves that carried out the crimes.

1970 - Nuclear Non-Proliferation Treaty (“NPT”)¹³

The NPT is based on a central bargain, that the NPT non-nuclear weapon states agree never to acquire nuclear weapons and the NPT nuclear weapons states agree in exchange, to share the benefits of peaceful nuclear technology and to pursue disarmament aimed at the ultimate elimination of their arsenals. There are five nuclear weapons states under the Treaty, being the permanent members of the UN Security Council, US, Russia, UK, France and China. Countries that also are believed to have nuclear weapons are either not members of the NPT or have withdrawn, for example, India and Pakistan, the rogue state of North Korea and Israel.

1970 - USA - Bank Secrecy Act¹⁴

The Bank Secrecy Act of 1970 (or BSA, or otherwise known as the Currency and Foreign Transactions Reporting Act) requires financial institutions in the US to assist US government agencies to detect and prevent money laundering. Specifically, the act required financial institutions to keep records of cash purchases of negotiable instruments, and file reports of cash purchases of these negotiable instruments of more than \$10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. The BSA was originally passed in 1970, and amended several times since then, most notably by the USA Patriot Act. The BSA is sometimes referred to as an "Anti-Money Laundering" ("AML") law or jointly as "BSA/AML".

1971 - Convention for the Suppression of Unlawful Seizure of Aircraft (the “Hague Convention”)¹⁵

Signed at The Hague on 16 December 1970 and entering into force on 14 October 1971, the Convention for the Suppression of Unlawful Seizure of Aircraft contains 14 articles relating to hijacking as well as guidelines for what is expected of governments when dealing with hijackings.

1971 - Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (the “Montreal Convention”)¹⁶

Signed on 23 September 1971 in Montreal, the Convention deals with acts other than those covered by the 1963 Tokyo and the 1970 Hague Convention. Also known as the Montreal Convention, it defined a wide spectrum of unlawful acts against the safety of civil aviation. The Convention contained detailed provisions on jurisdiction, custody, prosecution and extradition of the alleged offender going further than the Hague Convention and the Tokyo Convention. The Convention attempted to establish a form of universal jurisdiction over the offender.

1971 - Convention on Psychotropic Substances¹⁷

The 1971 Convention extended international control to cover synthetic psychotropic substances, such as LSD and MDMA, as well as their precursor chemicals. There was no system of estimates in the 1971 Convention, but it did retain a statistical returns system similar to that of the 1961 Single Convention. Its control system was therefore considerably weaker than that of the 1961 Single Convention. This was due in large part to the strong pharmaceutical lobby keen to draw a balance between, on the one hand, using controls to protect the interests of established producers from new competitors, and on the other, continuing to expand production and worldwide marketing by ensuring that such controls did not go too far.

1972 - The Biological Weapons Convention¹⁸

This was the result of prolonged efforts by the international community to extend the prohibition already on use of biological weapons, contained in the 1925 Geneva Protocol, to cover also possession and development.

1973 - Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents¹⁹

The Convention was adopted in 1973 and provided that states must make attacks upon diplomats for a crime in internal law, and obliged them to extradite or prosecute offenders. However, in exceptional cases, a diplomat could be arrested or detained on the basis of self-defence or in the interests of protecting human life.

1975 - Convention on International Trade in Endangered Species of Wild Flora and Fauna (CITES or the “Washington Convention”)²⁰

This Convention was drafted as a result of a resolution adopted in 1963 at a meeting of members of the International Union for Conservation of Nature (IUCN). Its aim was to ensure that international trade in specimens of wild animals and plants did not threaten the survival of the species in the wild, and it accorded varying degrees of protection to more than 33,000 species of animals and plants.

1977 - Switzerland - The agreement on the Swiss banks’ Code of Conduct with regard to the Exercise of Due Diligence (CDB) (revised latest 2008)²¹

Established in 1977, the Swiss Banks' Code of

Conduct on the Exercise of Due Diligence (CDB) set out detailed rules on identifying bank customers including in particular establishing the beneficial owner of every account where appropriate, document verification, clarification of the background of unusual transactions and the establishment and maintenance of records of transactions. Since its enactment the Code has been revised on a five-year cycle, the latest being the 2008 revision. Failure to comply with CDB rules triggers financial penalties. Whilst the Code is to be distinguished from the financial due diligence process as regulated in the Swiss Money Laundering Act and Money Laundering Ordinance, the CDB is effectively a minimum standard required to be complied with by Swiss Banks. The CDB in 1977 was perhaps the first of its kind, in setting out detailed KYC requirements for financial institutions to avoid money laundering risks.

1977 - USA Foreign Corrupt Practices Act (FCPA)²²

The FCPA is a law known primarily for two of its main provisions, one that addresses accounting transparency requirements under the Securities Exchange Act of 1934 requiring companies to maintain proper books and records and another concerning bribery of foreign officials. The anti-bribery provisions of the FCPA prohibit issuers, domestic concerns, and any person from making use of interstate commerce corruptly, in furtherance of an offer or payment of anything of value directly or indirectly to a foreign official, foreign political party, or candidate for political office, for the purpose of influencing any act of that foreign official in violation of the duty of that official, or to secure any improper advantage in order to obtain or retain business

1983 - International Convention against the Taking of Hostages (The “Hostage Convention”)²³

This Convention was adopted by the General Assembly of the UN in 1979, and entered into force in 1983. It provides that "any person who seizes or detains and threatens to kill, to injure, or to continue to detain another person in order to compel a third party, namely, a State, an international intergovernmental organisation, a natural or juridical person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage commits the offence of taking of hostage within the meaning of this Convention".

1984 - USA - Insider Trading Sanctions Act²⁴

The Insider Trading Sanctions Act of 1984 provided that, if the SEC believed that any person had bought or sold a security while in possession of material non-public information, as well as those who provided information not generally available to the public, the SEC may bring an action in US district court to seek a civil penalty. The penalty may be up to three times the profit gained or loss avoided. The Act also provides for criminal fines to be levied.

1985 - UK Company Securities (Insider Dealing) Act²⁵

The UK Company Securities (Insider Dealing) Act prohibited persons who had access to material non-public information by virtue of their position with a company (including directors, officers, employees, and various kinds of agents of the company) from trading in the securities of the company while in possession of such information. These insiders were also prohibited from making selective disclosure of such information to others ('tipping'); and it prohibited their tippees from trading on basis of such inside information. The Act also prohibited persons in possession of non-public information about a proposed takeover of a company from trading in that company's stock. The Act established only criminal liability, and its prohibitions applied only to individuals who acted while knowingly in possession of inside information. The Act was replaced by the Criminal Justice Act 1993 which represented an extension of the basis of liability for the insider dealing offence and contained a wider definition of 'securities' and 'insider' than the 1985 Act and the nature of the inside information necessary to impose liability was also altered.

1986 - USA - Money Laundering Control Act²⁶

The Money Laundering Control Act of 1986 made money laundering a federal crime. It consists of two sections, It for the first time criminalised money laundering. It prohibited individuals from engaging in a financial transaction with proceeds that were generated from certain specific crimes, known as "specified unlawful activities" (SUAs). There was no minimum threshold of money, nor was there the requirement that the transaction succeed in actually disguising the money. Moreover, a "financial transaction" has been broadly defined, and need not involve a financial institution, or even a business. Merely passing money from one person to another, so long as it is done with the intent to disguise the source, ownership, location or control of the money, has been deemed a financial transaction under the law.

1987 - Convention on the Physical Protection of Nuclear Material (CPPNM)²⁷

This Convention on the Physical Protection of Nuclear Material was adopted in 1979 in Vienna, Austria and entered into force in 1987. The Convention is deposited with the International Atomic Energy Agency. In 2005 a diplomatic conference was convened to amend the CPPNM and strengthen its provisions. The US Department of State said that: the Convention provided for certain levels of physical protection during international transport of nuclear material. It also established a general framework for cooperation among states in the protection, recovery, and return of stolen nuclear material. Further, the Convention lists certain serious offenses involving nuclear material which state parties are to make punishable and for which offenders shall be subject to a system of extradition or submission for prosecution.

1988 - Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation²⁸

Signed in Montreal in 1988, the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation adds to the definition of "offence" given in the Montreal Convention of 1971: unlawful and intentional acts of violence against persons at an airport serving international civil aviation which cause or are likely to cause serious injury or death and such acts which destroy or seriously damage the facilities of such an airport or aircraft not in service located thereon or disrupt the services of the airport. The qualifying element of these offences is the fact that such an act endangers or is likely to endanger safety at that airport. These offences are punishable by severe penalties, and States are obliged to establish jurisdiction over the offences not only in the case where the offence was committed in their territory but also in the case where the alleged offender is present in their territory and they do not extradite him to the state where the offence took place.

1988 - BIS - Basel Committee on Banking Supervision Prevention of Criminal use of the Banking System for the purposes of Money Laundering²⁹

The Basel Committee issued its first paper on money laundering publishing a statement of ethical principles which encouraged bank management to put in place effective procedures to ensure that all persons conducting business with their institutions are properly identified, that transactions that do not appear legitimate are discouraged, and that co-operation with law enforcement agencies is achieved.

1988 - UN Convention against illicit traffic in narcotic drugs and psychotropic substances (the "Vienna Convention")³⁰

The 1988 Vienna Convention was the first international convention to address money laundering and is relied upon by later conventions and treaties, building on the commitments made. Whilst the Convention focussed on drug trafficking it clearly recognised the links to organised and other forms of serious crimes. The Convention is also important because for the first time it included as a purpose to "deprive persons engaged in illicit traffic from the proceeds of their criminal activities and thereby eliminate their main incentive for so doing". Article 3 of the Convention calls on States to incriminate three types of activities. First the conversion or transfer of drug derived property for the purpose of concealing or disguising the illicit origin of the property" or second the "concealment or disguise" of drug derived property such as its nature, source, location, dispositions, movement, ownership and rights

to it and third the "acquisition, possession or use" of property, knowing at the time of receipt, that such property was derived from offences related to illicit drug trafficking. Although the term "money laundering" itself was not used, these three elements constitute the basis for what is today the crime of money laundering. The Convention includes additional measures in relation to jurisdiction, confiscation, extradition, mutual legal assistance and co-operation between states. Almost all countries in the world have signed and ratified the Vienna Convention.

1989 - European Community Directive Coordinating Regulations on Insider Trading³¹

Adopted in 1989, the EC Directive Coordinating Regulations on Insider Trading defined "inside information" as information of a "precise nature" about a security or issuer which has not been made public which, if it were made public, "would likely have a significant effect on the price" of the security (Article 1); It prohibited insiders from taking advantage of inside information (Article 2); It prohibited insiders from tipping or using others to take advantage of inside information (Article 3); It applied its prohibitions to tippees with "full knowledge of the facts" (Article 4); and it required all members to enact legislation complying with the Directive by June 1992. A fundamental difference between the EC Directive and the US prohibition against insider trading under Section 10b and Rule 10b-5 as developed by the US courts, is that the Directive did not require that the insider trader breach a fiduciary duty to the source of the information for liability to attach.

1990 - FATF 40 Recommendations First Issue³²

In April 1990, less than one year after the FATF was created, they issued a report containing a set of Forty Recommendations, which provided a comprehensive plan of action needed to combat the misuse of financial systems by persons laundering drug money. The 40 Recommendations provided a complete set of counter-measures against money laundering covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation. They set out the essential measures that countries should have in place to: identify the risks, and develop policies and domestic coordination; pursue money laundering, terrorist financing and the financing of proliferation; apply preventive measures for the financial sector and other designated sectors; establish powers and responsibilities for the competent authorities (for example, investigative, law enforcement and supervisory authorities) and other institutional measures; enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and facilitate international cooperation. Since the 1990 40 Recommendations, FATF has revised them in 1996, 2003 and 2012, added 8 Special Recommendations on Terrorism Financing in 2001 and a ninth in 2004 re-issuing most recently a consolidated set of 40 Recommendations in 2012. Together the

Forty Recommendations and Special Recommendations set out the principles for action and allow countries a measure of flexibility in implementing these principles according to their particular circumstances and constitutional frameworks. Both sets of FATF Recommendations are intended to be implemented at the national level through legislation and other legally binding measures.

1991 EU First Money Laundering Directive³³

The EU First Money Laundering Directive was enacted in response to growing concerns that the developing financial system could be used for criminal purposes and it recognised the possible susceptibility of professionals to money laundering activities. The First Directive provided the initial framework for the subsequent Second and Third Directives. It established key preventative measures such as customer/client identification, record-keeping and central methods of reporting suspicious transactions. It was passed to ensure a universal approach was adopted by EU member states to combat the problem of money laundering. The First MLD requirements stated that: (i) due diligence checks must be carried out by all credit and financial institutions before entering into any business relationship or before conducting any transaction over a certain threshold; (ii) all collated identification documents, evidence and existing records collected as part of the due diligence checks must be kept for at least five years by credit and financial institutions; (iii) there must be close international co-operation and harmonisation between credit and financial institutions and their supervisory authorities and the establishment of a mandatory central system of reporting; (iv) the confidentiality rules regarding customer information should be toned down in relation to disclosing suspected money laundering offences to the authorities; and (v) special protection should be afforded to credit and financial institutions, their employees and their directors who have to breach confidentiality rules in order to make the disclosure.

1992 - Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation³⁴

The main purpose of the convention is to ensure that appropriate action is taken against persons committing unlawful acts against ships. These include the seizure of ships by force; acts of violence against persons on board ships; and the placing of devices on board a ship which are likely to destroy or damage it. The convention obliges contracting governments either to extradite or prosecute alleged offenders. It was adopted in 1988 and entered into force on March 1, 1992. Protocols were added in 2005.

1993 - Convention on Biological Diversity (CBD)³⁵

The Convention on Biological Diversity (CBD), negotiated under the auspices of the UN Environment Programme (UNEP), was adopted in 1992 and entered into force in 1993. Its aims are the conservation of biological diversity, the sustainable use of biological

resources, and the fair and equitable sharing of benefits arising from the use of genetic resources. One of the major challenges facing the Convention on Biological Diversity is the communication of research results in a way that provides the policy makers, their advisors, the scientific community and other stakeholders with helpful insights. To help implement the Convention on Biological Diversity, the EU launched its own Biodiversity Strategy in 1998. It contained general measures to promote conservation and the sustainable use of biological diversity, in line with Article 6 of the CBD. Four major Biodiversity Action Plans were initiated in 2001, on the conservation of natural resources, agriculture, fisheries and economic and development co-operation. In 2001, Heads of member states adopted a Sustainable Development Strategy (SDS) in Gothenburg, Sweden. The SDS strengthened the Biodiversity Strategy by adopting the target to 'halt' the decline in biodiversity by 2010 inside the EU. In July 2002, the EU adopted its Sixth Environment Action Programme ('Environment 2010: Our Future, Our Choice'), which established a ten-year framework for priorities under the SDS. The programme addresses nature and biodiversity protection.

1993 - The Chemical Weapons Convention³⁶

This Chemical Weapons Convention essentially mirrors the Biological Weapons Convention 1975, but also provides for the destruction and verification of all Chemical stockpiles. As of November 2011, around 71% of the declared stockpiles of chemical weapons had been destroyed. Several countries, that are not members are suspected of having chemical weapons, especially North Korea and Syria, whilst others including Sudan are accused by some of not declaring accurately their stockpiles. The 2 countries with the largest declared stockpiles, Russia and the USA are in the process of destroying them, with the former at around 57% and the latter at 90% completed.

1996 - USA Inter-American Convention against Corruption³⁷

Adopted in 1996, the OAS Convention represented a regional consensus about what states should do in the areas of prevention, criminalisation, international cooperation and asset recovery. The Convention has been ratified by all members of the OAS. It covers corruption in the public sector, both on demand and supply. It gives a wide and inclusive interpretation to what constitutes "corruption offences" including bribery, domestic and foreign; illicit enrichment; money laundering and concealment of property. Measures adopted to curb bribery include preventive measures (creating and enforcing codes of conduct), criminalisation and regional assistance cooperation measures, as well as provisions on recovery of assets. Obligations towards the Convention are a combination of mandatory and discretionary provisions. For monitoring, a committee of experts has been established that is to conduct technical analysis of the implementation of the Convention by parties.

1996 - FATF 40 Recommendations - Revised³⁸

Initially developed in 1990, the 40 Recommendations were revised for the first time in 1996 to reflect evolving money laundering trends and techniques, broaden their scope well beyond drug-money laundering, and to anticipate potential future threats. In 1996, the FATF issued a series of interpretative notes designed to clarify their application.

1997 - International Convention for the Suppression of Terrorist Bombings (Terrorist Bombings Convention)³⁹

The International Convention for the Suppression of Terrorist Bombings was designed to criminalise the unlawful and intentional use of explosives in public places with the intention to kill, to injure, or to cause extensive destruction to compel a government or an international organisation to do or to abstain from doing some act. It also sought to promote police and judicial cooperation to prevent, investigate and punish those acts.

1998 - UN Political Declaration and Action Plan against Money Laundering⁴⁰

The UN's Political Declaration and Action Plan against Money Laundering was adopted in 1998. It urged jurisdictions and regions throughout the world to apply the following principles by 2003: 1. Establishment of a legislative framework to criminalise the laundering of money derived from serious crimes in order to provide for the prevention, detection, investigation and prosecution of the crime of money laundering; 2. Identification, freezing, seizure and confiscation of the proceeds of crime; and 3. Establishment of an effective financial and regulatory regime to deny criminals and their illicit funds access to national and international financial systems, thus preserving the integrity of financial systems worldwide and ensuring compliance with laws against money laundering.

1998 - EU Council of Europe Criminal Law Convention & Civil Law Convention⁴¹

These EU Council of Europe Criminal Law Convention & Civil Law Conventions were both adopted in 1998. The former Convention represents a European regional consensus on what states should do in the areas of criminalisation and international cooperation with respect to corruption. The Convention covers the public sector and private sector (private-to-private) corruption and covers a broad range of offences including bribery (domestic and foreign), trading in influence, money laundering and accounting offences. Penalty ranges from criminalisation to recovery of assets, with regional co-operation. The latter Convention was the first attempt to define common international rules in the field of civil law and corruption. In particular, it provides for compensation for damages as a result of acts of corruption. While it also covers the public and private sector, a broad scope is given to the Convention covering the "requesting, offering, giving or accepting of a bribe or any other undue advantage or the prospect

thereof". Civil law remedies for injured persons include compensation for damages from corruption; invalidity of corrupt contracts; whistleblower protection. The monitoring mechanism is the same as adopted for the Criminal Convention. The Convention called for mandatory provisions with no reservations allowed in respect of any provision of the Convention.

1998 - BIS - Basel Committee on Banking Supervision - "Prevention of criminal use of the banking system for the purpose of money laundering"⁴²

The BCBS issued a general statement of ethical principles which encouraged banks' management to put in place effective procedures to ensure that all persons conducting business with their institutions are properly identified; that transactions that do not appear legitimate are discouraged; and that cooperation with law enforcement agencies is achieved. The Committee considered that the first and most important safeguard against money laundering is the integrity of banks' own managements and their vigilante determination to prevent their institutions becoming associated with criminals or being used as a channel for money laundering. The statement is intended to reinforce those standards of conduct.

1999 - OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions⁴³

The Convention was signed on 17 December 1997 and came into force on 15 February 1999. It aimed at reducing corruption in developing countries by encouraging sanctions against bribery including foreign public offices in international business transactions carried out by companies based in the Convention member countries. Its goal is to create a truly level playing field in today's international business environment. Countries that have signed the Convention are required to put in place legislation that criminalises the act of bribing a foreign public official. The OECD has no authority to implement the convention, but instead monitors implementation by participating countries. Countries are responsible for implementing laws and regulations that conform to the Convention and therefore provide for enforcement.

1999 - International Convention for the Suppression of the Financing of Terrorism ("The Terrorist Financing Convention")⁴⁴

The Convention was designed to criminalise acts of those who finance terrorist activities and to promote police and judicial cooperation to prevent, investigate and punish financing those acts. Article 2.1 defines the crime of terrorist financing as the offence committed by "any person" who "by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an act "intended to cause death or serious bodily injury to a civilian, or to any other person

not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act." State parties to this treaty committed themselves also to freezing and seizure of funds intended to be used for terrorist activities, to share the forfeited funds. Moreover, states committed themselves not to use bank secrecy as a justification for refusing to cooperate.

1999 - USA Financial Services Modernisation Act Gramm-Leach-Bliley⁴⁵

"Glass-Steagall" was one of the many necessary measures taken in 1933 by President F D Roosevelt and the Democratic Congress to deal with the aftermath of the Great US Stock Market Crash. The Policy response was to erect a wall between investment banking and commercial banking (see above). In the 1990s, as another bull market took hold, momentum built to overturn Glass-Steagall. Commercial banks overeager to get into high margin businesses, saw commercial banks with their massive customer bases as important distribution channels for stocks, mutual funds and other financial profits. To many it was the 1998 acquisition by Sandy Weill's Travellers which owned Salomon Smith Barney of Citicorp, which lobbied hard for changes that may have made a difference. It had been given a temporary waiver in 1988 in order to allow the acquisition to go ahead. The year after the "Financial Services Modernisation Act" was passed effectively deleting the prohibition on commercial banks owning investment banks and vice versa. In reforming the US Financial Services Industry to allow consolidation the Act rejected appeals to introduce comprehensive AML standards into law, particularly KYC and beneficial owners' standards for all relevant accounts.

2000 - Convention against Transnational Organised Crime (the "Palermo" Convention)⁴⁶

The Convention provided for measures to prevent and combat transnational organised crime and is further supplemented by three protocols which target specific areas and manifestations of organised crime: Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children; Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing and Trafficking in Firearms.

2001 - EU Second Money Laundering Directive⁴⁷

The Second MLD amended and updated the First MLD on the prevention of the use of the financial system for the purpose of money laundering. The aim of the Second MLD was to refine the existing provisions created by the First MLD and to plug the gaps in the legislation highlighted by the 40 Recommendations, suggested by the FATF. The Second MLD adopted a broader definition of money laundering, taking into account underlying offences such as corruption and thus expanding the predicate offences. The Second MLD

also clarified that currency exchange offices, money transmitters and investment firms were included within the scope of the directive as they were susceptible to money laundering also. In addition, the Second MLD added the authority to identify, trace, freeze, seize and confiscate any property and proceeds linked to criminal activities. Moving on from the First MLD, the Second MLD touched upon the possibility of the Directive becoming applicable to lawyers participating in financial or corporate transactions. The proposition to extend the provisions of the Directive to the legal profession was met with fierce opposition by the European Parliament. It was due to fears that it would encroach on client confidentiality rules and could potentially violate the integrity of court proceedings. A compromise was reached and the scope of the Second Directive was not extended to cover professionals, such as lawyers. Thus, lawyers were exempt from reporting information received in the course of defending or representing a client.

2001 - BIS - Basel Committee on Banking Supervision its Customer Due Diligence Paper for Banks⁴⁸

In 1999 a Committee working group made findings that led the Committee to conclude that there existed great deficiencies in a large number of countries' know-your-customer (KYC) policies for banks. Judged from a supervisory perspective, KYC policies in some countries had significant gaps and in others they were considered non-existent. Even among countries with well-developed financial markets, the extent of KYC robustness varied. Consequently, the Basel Committee asked the Working Group on Cross-border Banking to examine the KYC procedures currently in place and to draw up recommended standards applicable to banks in all countries. The resulting paper was issued in 2001 setting out a KYC framework that would become the benchmark for supervisors to establish national practices and for banks to design their own programmes. The paper outlined four essential elements necessary for a sound KYC programme. These elements are: (i) customer acceptance policy; (ii) customer identification; (iii) on-going monitoring of higher risk accounts; and (iv) risk management. The principles laid down have been accepted and widely adopted by jurisdictions throughout the world as a benchmark for commercial banks and a good practice guideline for other categories of financial institution.

2001 - USA - Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act (the "PATRIOT" Act)⁴⁹
The Patriot Act was signed into law by President George W. Bush on 26 October 2001. The Act, a response to the terrorist attacks of 11 September 2001, dramatically reduced restrictions in law enforcement agencies' gathering of intelligence within the US, expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and broadened the discretion

of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts. The Act also expanded the definition of terrorism to include domestic terrorism, thus enlarging the number of activities to which the USA Patriot Act's expanded law enforcement powers could be applied. The Act also amended portions of the Money Laundering Control Act of 1986 and the Bank Secrecy Act of 1970 (detailed above). It criminalised the financing of terrorism and augmented the existing BSA framework by strengthening customer identification procedures; prohibited financial institutions from engaging in business with foreign shell banks; required financial institutions to have due diligence procedures (and enhanced due diligence procedures for foreign correspondent and private banking accounts); improved information sharing between financial institutions and the US government by requiring government-institution information sharing and voluntary information sharing among financial institutions; expanded the Anti-Money Laundering programme requirements to all financial institutions; increased civil and criminal penalties for money laundering; provided the Secretary of the Treasury with the authority to impose "special measures" on jurisdictions, institutions, or transactions that are of "primary money laundering concern"; facilitated records access and required banks to respond to regulatory requests for information within 120 hours; required federal banking agencies to consider a bank's AML record when reviewing bank mergers, acquisitions, and other applications for business combinations. In 2011, President Obama signed a four-year extension of three key provisions in the USA Patriot Act: roving wiretaps, searches of business records and conducting surveillance of "lone wolves", individuals suspected of terrorist-related activities not linked to terrorist groups.

2001 - FATF 8 Special Recommendations on Terrorism Finance (later to be become 9 Special Recommendations in 2004)⁵⁰

In October 2001, following the September 11 terrorist attacks in the US, the FATF issued the Eight Special Recommendations to deal with the issue of terrorism financing. These Recommendations contained a set of measures aimed at combating the funding of terrorist acts and terrorist organisations, and are complementary to the 40 Recommendations. The continued evolution of money laundering techniques led the FATF to revise the FATF standards comprehensively in June 2003 and in October 2004 the FATF published a ninth recommendation to its list of Special Recommendations on Terrorist Financing. The ninth recommendation called for countries to adopt measures to detect and prevent the physical cross-border transportation of money related to terrorist financing and money laundering. See below for Anti-Money Laundering and counter-terrorist financing efforts.

2002 - USA - Act to Protect Investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other

purposes; also known as "Public Company Accounting Reform and Investor Protection Act" and "Corporate and Auditing Accountability and Responsibility Act" "Sarbanes Oxley" or "SOX"⁵¹
In late 2001, Enron collapsed into bankruptcy, taking Arthur Andersen down with it. Between then and mid-2002, Xerox, Adelphia, Worldcom, and Tyco were among the companies in the headlines for executive misconduct and multi-billion dollar restatements. The Sarbanes-Oxley Act sought to strengthen accountability by auditors, executives, and boards of directors and to improve communication of companies' activities and financial condition to investors. The law stressed that companies disclose 'on a rapid and current basis' any material changes in operations or financial condition.

2003 - FATF 40+8 Recommendations - Revised⁵²

The FATF Recommendations were revised a second time in 2003. The scope of the recommendations were amended to include designated non-financial businesses and professionals. Designated non-financial businesses and professionals are defined by the FATF to include Casinos, Real Estate Agents, Dealers in Precious Stones and Metals, and Lawyers Accountants and Trust and Company Service Providers. The 2003 amendments applied, for the first time, customer due diligence and record keeping practices to Designated Non-Financial Businesses and Professionals. They are required to report transactions suspected of being linked to money laundering to the designated authorities. In the case of lawyers, the FATF recommended that lawyers be excused from this responsibility if their knowledge or suspicions arise as a result of legal professionally privileged circumstances. The 2003 amendments revised the recommendations to include the FATF's enhanced counter terrorist financing mandate.

2003 - UN Convention against Corruption (UNCAC)⁵³

The Convention was adopted in Mexico, on 31 October 2003. The Convention is the first legally binding international anti-corruption instrument. In its eight Chapters and 71 Articles, the UNCAC obliges its States Parties to implement a wide and detailed range of anti-corruption measures affecting their laws, institutions and practices. The Convention covers five main areas: 1) Prevention - measures such as the establishment of anticorruption bodies and enhanced transparency in the financing of election campaigns and political parties address both the public and private sectors. Requirements are also established for the prevention of corruption in the judiciary and in public procurement. The Convention calls on countries to actively promote the involvement of nongovernmental and community based organisations, as well as other elements of civil society, to raise public awareness of corruption. 2) criminalisation and law enforcement measures -

countries are required to establish criminal and other offences to cover a wide range of acts of corruption. This includes not only basic forms of corruption, such as bribery and the embezzlement of public funds, but also trading in influence and the concealment and "laundering" of the proceeds of corruption. 3) International co-operation - countries agree to cooperate in the fight against corruption, including prevention and investigation activities, and the prosecution of offenders. The Convention also binds countries to render specific forms of mutual legal assistance in gathering and transferring evidence for use in court and to extradite offenders. Countries must also undertake measures to support the tracing, freezing, seizure and confiscation of the proceeds of corruption. 4) asset recovery - This is an important issue for many developing countries where high-level corruption has plundered the national wealth, and where resources are badly needed for reconstruction and the rehabilitation of societies under new governments. Measures include the prevention and detection of transfers of illicitly acquired assets, the recovery of property, and the return and disposition of assets. 5) Implementation mechanisms - the Convention needs 30 ratifications to come into force. A Conference of the States Parties is established to review implementation and facilitate activities required by the Convention.

2003 - The Trafficking in Persons Protocol Palermo Protocol (Protocol to the Convention against Transnational Organised Crime 2000)⁵⁴

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children, also referred to as the Trafficking Protocol or UN TIP Protocol, is a protocol to the Convention against Transnational Organised Crime. The Trafficking Protocol entered into force on 25 December 2003. The Protocol commits states to prevent and combat trafficking in persons, protecting and assisting victims of trafficking and promoting cooperation among states in order to meet those objectives.

2003 - African Union Convention on Preventing and Combating Corruption⁵⁵

Adopted in 2003, this African Union Convention on Preventing and Combating Corruption has been ratified by 53 African countries. It covers the public and the private sector. Offences covered are bribery (domestic or foreign), diversion of property by public officials, trading in influence, illicit enrichment, money laundering and concealment of property. All provisions are mandatory including those on private to private corruption. The Convention provides for prevention, criminalisation, regional cooperation and mutual legal assistance as well as the recovery of assets. The follow-up mechanism provided for in Article 22 calls for an Advisory Board which has broad responsibilities for promoting anti-corruption work, collecting information on corruption in Africa, developing methodologies, advising governments, developing codes of conduct for public officials, and building partnerships. In addition it

is required to submit a report to the Executive Council on a regular basis on the progress made by each State Party in complying with the provisions of the African Union Convention. States parties are required to report to the Board on their progress in implementing the Convention on an annual basis. They are also required to ensure and provide for the participation of civil society in the monitoring process.

2003 - BIS - Basel Committee on Banking Supervision issued a General Guide to account opening and customer identification⁵⁶

The Basel Committee on Banking Supervision in its paper on Customer Due Diligence for Banks published in October 2001 referred to the intention of the Working Group on Cross-border Banking to develop guidance on customer identification, being an essential element of an effective customer due diligence programme which banks needed to put in place to guard against reputational, operational, legal and concentration risks. It was also necessary in order to comply with Anti-Money Laundering legal requirements and a prerequisite for the identification of bank accounts related to terrorism. The Guide issued sets account opening and customer identification guidelines and a general guide to good practice based on the principles of the Basel Committee's Customer Due Diligence for Banks paper. This document did not cover every eventuality, but instead focused on some of the mechanisms that banks can use in developing an effective customer identification programme.

2004 - The Smuggling of Migrants by Land, Sea and Air - Palermo Protocol (Protocol to the Convention against Transnational Organised Crime 2000)⁵⁷

The Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the Convention against Transnational Organised Crime, was adopted by the UN in Palermo, Italy in 2000. It is also referred to as the Smuggling protocol. The Smuggling Protocol entered into force in 2004. The Protocol is aimed at the protection of rights of migrants and the reduction of the power and influence of organised criminal groups that abuse migrants. It emphasises the need to provide migrants with humane treatment, and the need for comprehensive international approaches to combating people smuggling, including socio-economic measures that address the root causes of migration.

2004 - BIS - Basel Committee on Banking Supervision issued its "Consolidated KYC Risk Management"⁵⁸

A key challenge in implementing sound KYC policies and procedures was how to put in place an effective groupwide approach. The legal and reputational risks for many banks are global in nature. As such, it is essential that each group develops a global risk management programme supported by policies that incorporate groupwide KYC standards. Policies and procedures at the branch or subsidiary level must be consistent with and supportive of the group KYC standards

even where for local or business reasons such policies and procedures are not identical to the group^s. The Committee issued its paper on this topic at the same time recognising that implementing effective KYC procedures on a groupwide basis is more challenging than many other risk management processes. Similar to the approach to consolidated credit, market and operational risk, effective control of consolidated KYC risk requires banks to coordinate their risk management activities on a groupwide basis across the head office and all branches and subsidiaries.

2005 - EU Market Abuse Directive ("MAD")⁵⁹

The EU's Market Abuse Directive was one of a number of EU initiatives implementing the EU's then Financial Services Action Plan for completing the single market for financial services. The Directive was agreed in 2003 and came into force in 2005. The aim of the Directive is to promote clean and efficient markets, regulated in a harmonised way throughout the EU. To this end the Directive requires member states to outlaw insider dealing and market abuse and to provide for timely disclosure of price sensitive information.

2005 - EU Third Money Laundering Directive⁶⁰

The Third Directive took into account FATF's revised Anti-Money Laundering and Counter Terrorist Financing Standards of 2003 was adopted in 2005 and became operative in December 2007. The scope of the Directive increased significantly. The requirements under "know your customer" have been replaced by an increased level of customer due diligence on a risk basis. The Directive specifies when customer due diligence should be carried out. It includes where a business relationship is established, transactions over €15,000 (previously €13,000) where there is a suspicion of money laundering or terrorist financing or where there are any doubts as to the veracity or adequacy of previously obtained ID. In order to complete CDD, an organisation must complete the following: (i) verify the customer's identity; (ii) identify any beneficial owner; (iii) obtain information on the purpose and nature of the business relationship; (iv) carry out ongoing monitoring. Simplified due diligence may be applied to specified low risk customers and products/services. While the identification and information requirements do not apply under simplified due diligence, ongoing monitoring does continue to apply. This broadens the previous exemption for designated bodies to include listed companies, public authorities, pensions and other low risk products. Enhanced due diligence is required where a customer does not present themselves for identification purposes, correspondent banking and Politically Exposed Persons (PEPs). The Directive also introduced requirements to address issues around the vulnerability of so called Designated Non-Financial Businesses and Professions such as lawyers, notaries, accountants, real estate agents, casinos and encompassing trust and company services, exceeding €15,000, and measures against the financing of terrorism.

2005 - Protocol against the Illicit Manufacturing and Trafficking in Firearms, their Parts and Components and Ammunition - Palermo Protocol (Protocol to the Convention against Transnational Organised Crime 2000)⁶¹

The Protocol supplements the UN Convention against Transnational Organised Crime (2000) and its purpose is to strengthen and unify international cooperation and to develop cohesive mechanisms to prevent, combat and eradicate the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition (firearms). Parties to the Protocol undertake to adopt and implement the strongest possible legislation to investigate and prosecute the offences stemming from the illicit manufacturing of and trafficking in firearms. Specific measures include the confiscation, seizure and destruction of firearms illicitly manufactured or trafficked; maintenance of records for at least 10 years in order to identify and trace firearms; the issuance of licences for the import and export of firearms; and the marking of firearms permitting identification of the manufacturer of the firearm, and the country of and year of import. Parties undertake to cooperate extensively at the bilateral, regional and international levels in order to achieve the Protocol's objectives including providing training and technical assistance to other Parties. Finally, Parties undertake to exchange relevant case-specific information on matters such as authorized producers, dealers, importers, exporters and carriers of firearms as well as information on organised criminal groups known to take part in the illicit manufacture and trafficking of such items.

2005 – Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation⁶²

In March 1988 a conference in Rome adopted the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation. The main purpose of the Convention was to ensure that appropriate action is taken against persons committing unlawful acts against ships. These include the seizure of ships by force; acts of violence against persons on board ships; and the placing of devices on board a ship which are likely to destroy or damage it. The 2005 Protocol to the Convention criminalised the use of a ship as a device to further an act of terrorism; criminalises the transport on board a ship various materials knowing that they are intended to be used to cause, or in a threat to cause, death or serious injury or damage to further an act of terrorism; criminalises the transporting on board a ship of persons who have committed an act of terrorism; and introduced procedures for governing the boarding of a ship believed to have committed an offence under the Convention.

2006 US Unlawful Internet Gambling Enforcement Act (UIGEA)

This Act made it a crime to knowingly accept most forms of payment "in connection with the participation of another person in unlawful internet gambling." As

a result of this Act most financial institutions refuse to permit credit card payments to be processed, for example, in US dollars and by US persons, striking a significant blow to those targeting the largest market for internet gambling.

2008 - Switzerland- Market Conduct Rules - FINMA Circular⁶³

According the Federal Act on Stock Exchanges and Securities Trading (Stock Exchange Act, or SESTA) which ensures transparency and the proper functioning of securities markets and equality in the treatment of investors, market developments must be monitored in a manner that ensures that insider trading, price manipulation or other legal violations may be detected (market surveillance). This Circular establishes rules on regulatory supervision pertaining to the market conduct of regulated market participants when engaging in securities transactions. It contains directives for preventing market manipulation and examples of accepted market practices. For example it states that, "Securities trading is to be based upon generally available or published information on securities and issuers or upon information derived therefrom. Information on securities and issuers is deemed generally available when it is published or disseminated in the media or via the usual information channels in the financial sector, or if it is derived from such information. All other information on securities and issuers is to be regarded as confidential. Misusing knowledge of confidential price sensitive information for securities transactions is not permissible (misuse of information). Information is deemed price sensitive where it is capable of significantly influencing the stock market price or the valuation of the respective securities. Specifically, such information pertains to circumstances that substantially impact a company's organisational structure, its executive and business management bodies, its course of business, its financial or earnings situation and thus its valuation, and is therefore capable of effecting material changes in the market price. These circumstances may be grounds for public disclosure and/or be subject to legal or self regulatory requirements to provide information (disclosure obligations pursuant to Article 20 SESTA or ad hoc publicity according to stock exchange regulations). The wrongful dissemination of confidential price-sensitive information or making references or recommendations based thereon pertaining to engaging in securities transactions are also deemed to constitute misuse of information. Rumours or vague hints are not deemed confidential information. However, knowingly spreading rumours or vague hints for the purpose of invoking same is not permissible. Taking advantage of the expected market reaction of market participants and of securities prices employing the knowledge of an impending announcement of investment recommendations ("scalping") is not permissible.

2009 - UK - FSA Code of Market Conduct⁶⁴

The UK broadened its attack on Market Abuse by

enacting section 118 of the Financial Services and Markets Act 2000 (FSMA), see above which was updated to also incorporate changes required arising out of the EU Market Abuse Directive (MAD) which came into force in July 2005 (see above). The MAD provisions were similar to those in a number of existing EU countries, in particular in the UK. The UK FSA issued a Code of Market Conduct (August 2009) which runs to 52 pages and covers seven market abuses spanning: i) insider dealing, ii) improper disclosure, iii) misuse of information, iv) manipulating transactions, v) manipulating and “fictitious” devices, vi) dissemination of information, and vii) misleading behaviour and distortion. These seven types of behaviour, as well as techniques and examples are set out by the FSA. The market abuse regime was introduced as a means of bringing more people who trade on inside information to justice. It sits alongside the criminal regime of insider dealing but operates with the lower standard of proof required for civil proceedings and potentially covers more transactions. However, in addition to these civil offences, both insider dealing and market manipulation remain criminal offenses. The market abuse regime covers: financial instruments (such as shares, warrants, futures, contracts for differences, options and debt instruments) traded on every regulated market in Europe (or for which an application for admission to trading has been made). In the UK, the relevant markets include the London Stock Exchange (both the full list and AIM), PLUS (the old OFEX) and commodity derivative markets; all transactions relating to those instruments even if they are carried out off-market. In certain circumstances, behaviour in respect of other, related instruments or underlying commodities is also caught, even if those instruments are not themselves traded on a regulated market. Behaviour involving securities traded on a foreign unregulated market may be caught if an option linked to them is traded in London.

2009 - OECD Recommendations for Further Combating Bribery of Foreign Public Officials in International Business Transactions⁶⁶

The OECD adopted on 25 May 2009 a new Recommendation to strengthen the role of tax authorities in the combat against bribery that succeeds to the former 1996 Recommendation. The 2009 Recommendation buildt on the powerful impact of the non-deductibility of bribes to foreign officials by requiring legislation or any other binding means to prohibit the tax deductibility of bribes to foreign public officials. A further Recommendation was issued on 9 December 2009, when the OECD marked the 10th anniversary of the entry into force of the OECD Anti-Bribery Convention. The new Recommendation was intended to enhance the ability of the OECD to prevent, detect and investigate allegations of foreign bribery and includes the Good Practice Guidance on Internal Controls, Ethics and Compliance. This Good Practice Guidance, contained in Annex 2 of the Recommendation, calls on companies to protect

themselves against the risks of foreign bribery by putting in place strict internal controls and establishing ethics and compliance programmes.

2010 - USA - The Foreign Account Tax Compliance Act (FATCA)⁶⁷

The Foreign Account Tax Compliance Act was enacted as part of the Hiring Incentives to Restore Employment (HIRE) Act, and is considered by the US Government as an important development in the US efforts to combat tax evasion by US persons holding investments in offshore accounts. The Act came into force on 1 January 2014. FATCA requires foreign banks to identify any American account holders and disclose their balances, receipts, and withdrawals to either (i) local IRS (to be completed) or (ii) directly to the US Internal Revenue Service (IRS), or be subject to a 30% withholding tax on income from US financial assets held by the banks. Owners of these foreign-held assets must report them on a new Form 8938 along with US tax returns if they are worth more than US \$50,000; a higher reporting threshold applies to overseas residents. The reporting requirements are in addition to reporting of foreign financial assets to the US Treasury Department, particularly the “Report of Foreign Bank and Financial Accounts” (FBAR) for foreign financial accounts exceeding US \$10,000 required under Bank Secrecy Act regulations issued by the Financial Crimes Enforcement Network (FinCEN).

2010 - UK - Bribery Act⁶⁸

The UK Bribery Act entered into force on 1 July 2011 and is described as “the toughest anti-corruption legislation in the world”. It has a wider range of offences than the US FCPA in that it covers all forms of bribery not just involving foreign public officials but also commercial bribery and it does not permit so called facilitation payments. The Act creates four offences: (i) giving a bribe; (ii) receiving a bribe; (iii) bribing a foreign public official; and (iv) failure by an organisation to prevent bribery. The penalties for committing a crime under the Act are a maximum of ten years imprisonment, along with an unlimited fine, and the potential for the confiscation of property as well as the disqualification of company directors. The Act has a near-universal jurisdiction, allowing for the prosecution of an individual or company with links to the UK, regardless of where the crime occurred.

2010 - Convention on Cluster Munitions (CCM)⁶⁹

The CCM is an international treaty that prohibits the use, transfer and stockpile of cluster bombs, a type of explosive weapon which scatters submunitions (bomblets) over an area. The Convention was signed in 2008 and came into force in 2010.

2010 - USA - Dodd-Frank Wall Street Reform Act⁷⁰

Named after its Democratic sponsors in Congress, Senator Chris Dodd and Representative Barney Frank, the law aimed at preventing a repeat of the 2008 global financial crisis. Dodd-Frank is the most comprehensive

US financial reform since the Glass-Steagall Act. Like Glass-Steagall, it sought to regulate the financial markets and make another economic crisis less likely. Banks were deregulated in 1999 by the Gramm-Leach-Bliley Act, which repealed Glass-Steagall. Dodd-Frank proposed the following areas of regulation set out in a 2000-page act which included sweeping new rules for banks, hedge funds and complex financial transactions called derivatives. The following are the most important: (i) Regulate credit cards, loans and mortgages. The Consumer Financial Protection Agency (CFPA) consolidated protection from many different agencies. It oversees credit reporting agencies, credit and debit cards, payday and consumer loans (but not auto loans from dealers). The CFPA regulated credit fees, including credit, debit, mortgage underwriting and bank fees. It protects homeowners in real estate transactions by requiring them to understand risky mortgage loans. It also requires banks to verify borrower's income, credit history and job status. The CFPA is under the US Treasury Department; (ii) Oversees Wall Street: the Financial Stability Oversight Council looks out for risks that affect the entire financial industry. It also oversees non-bank financial firms like hedge funds. If any of these companies get too big, it can recommend they be regulated by the Federal Reserve, which can ask it to increase its reserve requirement. This prevents another AIG from becoming too big to fail. The Council is chaired by the Treasury Secretary, and has nine members: the Fed, SEC, CFTC, OCC, FDIC, FHFA and the new CFPA; (iii) Volcker Rule: The Volcker Rule bans banks from using or owning hedge funds for the banks' own profit. That is because they would often use their depositors' funds to do so. Banks can use hedge funds for their customers only. Determining which funds are for the banks' profits and which funds are for customers has been difficult. Therefore, Dodd-Frank gave banks seven years to divest the funds. They can keep any funds if that are less than 3% of revenue. (iv) Regulate risky derivatives: Dodd-Frank required that the riskiest derivatives, like credit default swaps, be regulated by the SEC or the Commodity Futures Trading Commission (CFTC). In this way, excessive risk-taking can be identified and brought to policy-makers' attention before a major crisis occurs. A clearinghouse, similar to the stock exchange, must be set up so these derivative trades can be transacted in public. However, Dodd-Frank left it up to the regulators to determine exactly the best way to put this into place, which has led to a series of studies; (v) Bring hedge funds trades into the light: one of the causes of the 2008 global financial crisis was that, since hedge funds and other financial advisers were not regulated, no one knew what they were investing in or how much was at stake. That's why the Fed and other agencies thought the mortgage crisis would be confined to the housing industry. To correct for that, Dodd-Frank says that hedge funds must register with the SEC and provide date about their trades and portfolios so the SEC can assess overall market risk. States are

given more power to regulate investment advisers, since Dodd-Frank raises the asset threshold limit from US\$30mio to US\$100mio. (vi) Oversee credit rating agencies: Dodd-Frank created an Office of Credit Rating at the SEC to regulate credit ratings agencies like Moody's and Standard & Poor's. Many blame the agencies for over-rating some bundles of derivatives and mortgage-backed securities. This misled investors who didn't realise the debt was in danger of not being repaid. The SEC can require agencies to submit their methodologies for review, and can deregister an agency that gives faulty ratings; (vii) increase supervision of insurance companies: It created a new Federal Insurance Office under the Treasury Department, which identifies insurance companies like AIG that create risk to the entire system. It will also gather information about the insurance industry and make sure affordable insurance is available to minorities and other underserved communities. It will represent the US on insurance policies in international affairs. The new office will also work with the states to streamline regulation of surplus lines insurance and reinsurance. (viii) Reform the Federal Reserve: the Government Accountability Office(GAO) was allowed to audit the Fed's emergency loans during the financial crisis. It can review future emergency loans, when needed. The Fed cannot make an emergency loan to a single entity, like Bear Stearns or AIG, without Treasury Department approval, (although the Fed did work closely with Treasury during the crisis). The Fed must make public the names of banks that received these loans or TARP funds. Finally, both to ensure cooperation by financial insiders and fight corruption in the financial industry, the Dodd-Frank Act contains a whistle blowing provision, where persons with information about security violations can report information to the Government for a financial reward. US President Barack Obama, who signed the Act into law, said: “The American people will never again be asked to foot the bill for Wall Street's mistakes” but many in the financial services sector say the law and accompanying regulations are confusing, expensive and in some cases unworkable.

2011 - EU - Second Market Abuse Directive (“MAD 2”) - Proposals⁷¹

On 20 October 2011 the European Commission published proposals intended to update and strengthen the existing framework ensuring investor protection under the existing EU Market Abuse Directive issued in 2005 (see above). The European Parliament could adopt the proposals towards the end of this year, in which case it will be another two years after that for them to take effect - member states get 24 months to look at the implications for their domestic legislation in green). The proposals consist of a regulation on insider dealing and market manipulation (the “Regulation”) and a new directive on criminal sanctions for insider dealing and market manipulation (the “Directive”). The proposed update of the MAD is intended to ensure a consistent approach to market abuse issues

by regulators across the EU and provide an updated regulatory framework in order to keep pace with market developments. The Regulation introduces prohibitions, requirements and corresponding harmonised civil and administrative sanctions and powers intended to be directly applicable in each member state. Implementation of these measures in national legislation will therefore not be necessary once the Regulation has entered into force. ESMA shall provide further technical standards for amongst others insider lists and appropriate public disclosure of inside information. Minimum criminal sanctions are set out in the Directive, which is to be implemented on a national level. The Regulation broadens and clarifies the scope of the current market abuse framework by clarifying the definitions of "market manipulation" and "insider trading" and expanding the scope of European market abuse legislation to cover transactions in financial instruments traded on MTFs or OTFs and OTC transactions and in any related financial instruments traded on these markets or on a regulated market. The Regulation also clarifies which high frequency trading strategies constitute prohibited market manipulation. The Regulation sets out a broader definition of inside information than currently included in the MAD. Most notably, information regarded as relevant for the making of an investment decision by a reasonable investor, who regularly deals on the market and in certain financial instruments or related spot commodity contracts, is considered inside information. It will therefore no longer be necessary that such information is "price sensitive". While this expansion of the definition of inside information will broaden the scope of what is considered "insider dealing", it will not increase the quantity of information which must be disclosed to the public, due to the fact that the Regulation provides for an exemption to the obligation to disclose inside information which is not "price sensitive". The Regulation is intended to broaden the scope of the market abuse framework to cover those spot markets which are related to and have an effect on financial and derivative markets. Therefore the Regulation provides for broadened definitions of inside information and market manipulation with respect to commodity derivatives trading. The definition of inside information in relation to commodity derivatives will be aligned with the general definition of inside information and extended to cover price sensitive information which is relevant to the related spot commodity contract as well. The Regulation introduces a new definition for inside information relating to emission allowances. The prohibition on insider trading will also cover emissions allowances traded in auctions and auctioned products based thereon. Insider dealing: the Regulation explicitly prohibits "attempts to engage in insider dealing" and clarifies that both actual cancellations and attempts to cancel transactions are considered use of inside information which constitutes insider dealing. Market Manipulation: The Regulation introduces a new definition of "attempting to engage in market manipulation". In contrast to the MAD,

the Regulation no longer provides for an exemption for market manipulation which can be justified and which is performed in line with a market practice accepted by a national regulator and notified to ESMA. Also, the prohibition to manipulate the market under the Regulation is explicitly extended to cover spot commodity contracts. Furthermore, the Regulation provides for descriptions of acts which constitute market manipulation, including specific acts performed through algorithmic trading with respect to electronic media.

2012 - FATF 40 Recommendations⁷²

(International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation). In 2012, the Recommendations were again revised and included additional areas such as tax crimes. The main changes were: (i) Combating the financing of the proliferation of weapons of mass destruction through the consistent implementation of targeted financial sanctions when these are called for by the UN Security Council; (ii) Improved transparency to make it harder for criminals and terrorists to conceal their identities or hide their assets behind legal persons and arrangements; (iii) Stronger requirements when dealing with politically exposed persons (domestic PEPs); (iv) Expanding the scope of money laundering predicate offences by including tax crimes; (v) An enhanced risk-based approach which enables countries and the private sector to apply their resources more efficiently by focusing on higher risk areas; (vi) More effective international cooperation including exchange of information between relevant authorities, conduct of joint investigations, and tracing, freezing and confiscation of illegal assets; and (vii) Better operational tools and a wider range of techniques and powers, both for the financial intelligence units, and for law enforcement to investigate and prosecute money laundering and terrorist financing.

2012 - Switzerland - Stock Exchange Act (Amended)⁷³

Under pressure to step up the battle against insider trading, Switzerland has recently acted. The changes made to the Swiss Stock Exchange Act in 2012 essentially bring Switzerland into line with international requirements. Insider trading only became a crime in Switzerland in 1988, but the law was written far more narrowly than in other countries. Unlike the UK or the US, insider trading was an offense only in relation to the issue of new securities, mergers and acquisitions, but not ahead of earnings announcements, even when they contained potentially market-moving information. Moreover, Swiss law did not require mandatory jail time, and the fines were considered low by some to be an effective deterrent. Whilst standards were improved following the issuance of the Swiss Market Conduct Rules - FINMA Circular 2008, the new changes to the Act created new standards that aim to combat market abuse (insider dealing, front running, market manipulation and improper disclosure) even further

and more efficiently. In particular, insider trading and price manipulation is now prohibited for all market participants and both offences treated as crimes. The changes entered into force on 1 April 2013.

2012 - EU 4th AML Directive - Proposed and Funds Transfer Regulations Proposed⁷⁴

The EU proposals seek to update and improve the EU's existing 3rd AMLD and the Funds Transfers Regulation with the aim of further strengthening the EU's defences against money laundering and terrorist financing and ensuring the soundness, integrity and stability of the financial system. They reflect the latest FATF Recommendations issued in 2012. More specifically, both proposals provide for a more targeted and focussed risk-based approach. The proposed new Directive clarifies and reinforces the rules on customer due diligence and introduces new provisions to deal with domestic politically exposed persons. It goes beyond the FATF requirements by bringing within its scope all persons dealing in goods or providing services for cash payment of €7,500 which will lower the existing threshold set at €15,000. The proposed Directive also ensures a more comprehensive coverage of the gambling sector (in the light of concerns that the wide sector is vulnerable to money laundering) and includes an explicit reference to tax crimes. The proposals also consider increasing the sanctioning powers of the competent authorities by introducing a set of minimum principle-based rules to strengthen administrative sanctions and a requirement for them to coordinate actions when dealing with cross-border cases. Proposals to update the Regulation on information accompanying the transfers of funds has also been made in light of the revised international standards. Following are the key changes proposed: (i) Consolidating the risk-based approach: the new standards put more focus on the risk-based approach. This means that countries need to clearly understand the money laundering and terrorist financing risks which affect them, and adapt their Anti Money laundering/Counter Financing of Terrorism (AML/CFT) system to the nature of these risks – with enhanced measures where the risks are higher and the option of simplified measures where the risks are lower. Thus, countries will be able to target their resources more effectively and apply preventative measures that correspond to the risks of particular sectors or activities. A well-implemented risk-based approach means that the AML/CFT system will be more effective and less costly; (ii) Improving Transparency measures: there is a lack of transparency at the moment around the ownership of companies, making them potentially vulnerable to misuse by criminals and terrorists. The new Recommendations have strengthened transparency requirements. Reliable information available about the ownership and control of companies, trusts, and other legal persons or legal arrangements is required as well as more rigorous requirements on the information which must accompany electronic funds transfers. Measures to improve transparency, implemented on a global basis, will make it harder for criminals and terrorists to conceal their activities; (iii) Towards more effective international co-operation: with the increasing globalisation of money laundering and terrorist financing threats, the FATF has also enhanced the scope of international cooperation between government agencies, and between financial groups (for example, simplified extradition mechanisms). The revised Recommendations will allow more effective exchanges of information, tracing, freezing, confiscation and repatriation of illegal assets; (iv) Identification of clear operational standards: the FATF Recommendations concerned with law enforcement and FIUs have been expanded significantly. The revisions clarify the role and functions of the operational agencies responsible for combating money laundering and terrorist financing; and set out the range of investigative techniques and powers which should be available to them. In addition new threats and new priorities are covered by the new proposals as stated by the FATF Recommendations as follows: (i) Corruption & Politically Exposed Persons - the FATF Recommendations tighten the requirements on "politically exposed persons"; that is, people who may represent a higher risk of corruption by virtue of the positions they hold. The requirement to apply enhanced due diligence to foreign politically exposed persons has been expanded with the new Recommendations also applying to domestic politically exposed persons and international organisations, and to the family and close associates of all politically exposed persons – reflecting the methods used by corrupt officials and kleptocrats to launder the proceeds of corruption; (ii) Tax Crimes - the list of predicate offences for money laundering has been expanded to include tax crimes which are brought within the scope of the powers and authorities used to combat money laundering. This will contribute to better coordination between AML and tax authorities, and remove potential obstacles to international cooperation regarding tax crimes; and (iii) Terrorist Financing – the financing of terrorism remains a serious concern for the international community, and a major focus of the FATF. The Recommendations reflect both the fact that terrorist financing is a long-standing concern, and the close connections between Anti-Money Laundering measures and measures to counter the financing of terrorism. The two proposals are open now for consultation and will have to be adopted by the European Parliament and the Council of Ministers under the ordinary legislative procedure. Whilst the EU 3rd MLD allowed lighter customer due diligence measures to be applied in the case of financial institutions situated in EU/EEA countries, it also allowed and extended these lighter measures to institutions situated in third countries which impose AML requirements considered to be "equivalent" to those laid down in the Directive. Included as part of the definition of EU/EEA member states are of course EU member states themselves for example, Germany or Romania and Cyprus and EEA member states including Norway, Iceland and Liechtenstein. In addition also included are certain

overseas territories of member states, for example, the French overseas territories (Mayotte, New Caledonia, French Polynesia, Saint Pierre and Miquelon and Wallis and Futuna) and the Dutch ones, Aruba, Curacao, Saint Maarten, Bonaire, Saint Eustatius and Saba. The UK Crown Dependencies (Jersey, Guernsey, Isle of Man) are also to be considered as equivalent. True third country states considered as "equivalent" are: Australia; Brazil; Canada; Hong Kong; India; Japan; South Korea; Mexico; Singapore; Switzerland; South Africa and the US. The proposed 4th MLD will no longer promote a precise model or list of "equivalent" third countries, though EU/EEA countries will retain "equivalent status" and instead recommend financial institutions use their own risk based models and approaches.

2012 - EU - Directive on Freezing and Confiscation of The Proceeds of Crime - Proposed⁷⁵

In October 2012 the EU announced its intention to propose a directive on freezing and confiscation of proceeds of crime in the EU, alongside the European Parliament that has created a special Committee on organised crime, corruption and money laundering with a one year term. In the course of this one year the Committee will investigate the level of infiltration in EU's legal economy, public administration and financial systems of organised crime, including the mafia. Sonia Alfano MEP (ALDE, Italy), Parliament's rapporteur on this issue, said: "The establishment of an Anti-Mafia Committee in the European Parliament represents a real turning point in the history of EU policies. As for the Proposed Directive, "putting criminals in jail is only one part of this job. The other crucial work is making sure that crime does not pay - and ensuring that we empty criminals' pockets, and get their money back into the legal economy where it belongs. In times of crisis this is even more crucial", European Commissioner for Home Affairs, Cecilia Malmstrom said. The proposal referred to the total amount of criminal profits in 2009 which was approximately US\$2.1 trillion, according to UN estimates. There are no general estimates for the EU, but data for individual member states are instructive. In Italy, the profits of organised crime in 2011 were estimated at €150bio. In 2006 organised crime in the UK has earned £15bio. Compared to the profits of criminal activity, the amounts seized by governments are too modest - in 2009 seized assets amounted to €281mio in Germany, €185mio in France, €154mio in Britain, €50mio in the Netherlands. However, corruption costs the European taxpayer 1% of European gross domestic product annually, and only in Italy €6 bio annually sink into corruption schemes, according to the European Court of Auditors. The Commission concludes that "although regulated by EU and national laws, confiscation of criminal assets remains underdeveloped and underutilised." Therefore, the Directive provides a minimum set of rules to be applied by member states aimed at more efficient use of confiscation and freezing of assets acquired through criminal activity. In addition to the classical confiscation, resulting from a final criminal conviction,

the directive allows in a limited number of cases the application of: (i) confiscation of assets which are not directly linked to a specific crime, but which clearly result from similar criminal activities committed by the convicted person (extended confiscation); (ii) confiscation where assets have been transferred from the suspect to a third party; and (iii) confiscation of criminal assets where a criminal conviction is not possible because the suspect is deceased, permanently ill or has fled (non-conviction based confiscation). The new rules give prosecutors the right to freeze property in danger of being dissipated, hidden or transferred out of the jurisdiction with a view to getting a court ruling later. The member states are required to manage the frozen property in such a way that it does not lose value before being confiscated. To that end, they should create national centralised offices or equivalent mechanisms. At the same time, the directive instructs in details how the freezing and confiscation to be accompanied by guarantees that fundamental rights will be respected, particularly the presumption of innocence and the right of property. Member states are asked to keep comprehensive statistics and send them to the Commission each year to ensure evaluation of the effectiveness of their confiscation systems. The countries have two years after the Directive's entry into force to bring their legislation in line. Moreover, they should communicate to the Commission the texts of the main provisions of their national law in the covered by the directive areas.

2012 - USA - Advance Notice of Proposed Rulemaking on Customer Due Diligence (Expanding BO ID requirements) - Proposed⁷⁶

On 5 March 2012, FinCEN proposed for consultation a Customer Due Diligence (CDD) regulation ("CDD Proposal") that would be applicable to banks, and other FI's. For many US FI's, the CDD Proposal may significantly increase their overall Anti-Money Laundering (AML) compliance burden. Generally, the CDD Proposal consists of four elements, the key aspects of which include a proposed new beneficial owner definition that focuses on legal entities as accountholders, subject to limited potential exceptions. The proposal is expected to apply also to money services businesses, including providers of prepaid access, insurance companies, casinos, dealers in precious metals, stones and jewels and non-bank mortgage lenders or originators. Customer Identification and Verification: This element would require FI to identify, and on a risk-basis verify, the identity of each customer, to the extent reasonable, such that the institution can form a reasonable belief that it knows the true identity of each customer. FinCEN states that this element of the CDD Proposal is largely consistent with existing CIP obligations and has expressed the view that it would not impose any new or additional requirements. However, FinCEN notes that current customers, banks, governmental entities and publicly traded companies, are exempt from existing CIP requirements, and has requested comment on

whether the BO requirement should apply with respect to those exempt customers. Account Nature and Purpose: With respect to this element, FinCEN has proposed language that would require covered financial institutions to understand the nature and purpose of the account and expected activity associated with the account, for the purpose of assessing the risk and identifying and reporting suspicious activity. FinCEN states that this element of the CDD Proposal would not impose new or additional requirements on financial institutions given existing guidance in this area and the obligation to detect and report suspicious activity, however, no such obligation is express in existing regulations. Obtaining Beneficial Ownership Information: The third element of the CDD Proposal would expand upon the two limited situations where FIs are currently obligated by regulation to obtain beneficial ownership information—in connection with certain correspondent accounts for foreign banks and private banking accounts—by imposing what FinCEN describes as a categorical requirement, subject to potential limited exceptions, to obtain such information for all customers. Thus, under this element of CDD Proposal, financial institutions would be required to identify the beneficial owner(s) of all customers, and to verify the beneficial owners' identity pursuant to a risk-based approach. FinCEN states that it anticipates providing additional guidance regarding entities that would be considered both low- and high-risk customers, as well as guidance on what covered financial institutions should do in the event they are unable to identify or verify a beneficial owner. As part of this element of the CDD Proposal, FinCEN is considering a definition of a beneficial owner that would capture either: (i) each of the individual(s) who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity or otherwise owns more than 25% of the equity interests in the entity; or (ii) if there is no individual who satisfies the first prong, then the individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity or otherwise has at least as great an equity interest in the entity as any other individual. In addition, the individual with greater responsibility than any other individual for managing or directing the regular affairs of the entity also would be considered a beneficial owner. FinCEN anticipates that this definition would generally apply to legal entity customers and would not be used for purposes of current requirements (i.e., those imposed in connection with certain correspondent accounts for foreign banks and private banking accounts). In addition, recognizing that covered financial institutions may not have beneficial ownership information on existing customers, FinCEN is also considering whether and how the CDD Proposal would apply to existing customers of such institutions and is seeking comment on how a beneficial ownership identification requirement could be phased into ongoing CDD. Of interest to issuers of prepaid cards and other institutions that hold assets in omnibus or other intermediated accounts, FinCEN has requested comment on the difficulties associated with identifying beneficial owners in connection with such accounts. This aspect of the CDD Proposal will also be significant to various investment vehicles that maintain accounts at regulated institutions. FinCEN states that it is considering whether a potential explicit obligation to identify the beneficial owners of assets in those accounts should be based upon the financial institution's risk assessment of the customer, or whether a more specific obligation would be appropriate. With respect to account opening, FinCEN anticipates that, in general, the individual opening the account on behalf of a legal entity customer will identify its beneficial owner, and that covered financial institutions will generally be able to rely upon the beneficial ownership information presented by the customer. With respect to verification of that information, FinCEN has identified two possible approaches on which comment is sought. The first approach would require the financial institution to verify the identity of the individual identified by the customer as the beneficial owner of the account (i.e., verifying the existence of the identified beneficial owner). The second approach would require the financial institution to verify that the individual identified by the customer as the beneficial owner is indeed the beneficial owner of the customer (i.e., verifying the status of the identified individual), which is a much more challenging effort. In either case, FinCEN contemplates that the required procedures would need to be reasonable and practicable, and sufficient to form a reasonable belief that the financial institution knows the identity or status of the beneficial owner. Ongoing CDD: The fourth element of the CDD Proposal addresses ongoing due diligence with respect to customer relationships. Observing that due diligence is an ongoing obligation and requires financial institutions to have policies and procedures in place to maintain the accuracy of their customer risk profiles, FinCEN is proposing to require covered financial institutions to establish and maintain appropriate policies, procedures and processes for conducting on-going monitoring of all customer relationships and additional CDD as appropriate based on such monitoring for the purpose of the identification and reporting of suspicious activity. As with the first and second elements, FinCEN asserts that this element of the CDD Proposal is consistent with existing regulatory compliance obligations (e.g., requirements contained in the AML and suspicious activity reporting rules), and would not impose any new or additional requirements. In addition to the issues identified above on which comment has been requested, FinCEN has posed a variety of additional questions that are designed to assist FinCEN in better understanding what types of CDD information are currently collected, specifically in relation to beneficial ownership information, and under what circumstances the information is collected. These questions ask financial institutions to address, among other things, issues that may arise in the context of implementing the CDD Proposal, including any impact

on consumers and customers, and the processes through which institutions currently obtain beneficial ownership information. David Cohen, US DoT undersecretary for terrorism and financial intelligence, said recently that he expects the final rules to be released very shortly, but also suggested beneficial owner rules would require different degrees of inquiry in different circumstances. "There is a recognition that the financial sector is complex, and one-size-fits-all is not suitable here."

2013 - Switzerland - Federal Act on War Materials⁷⁷
Following Switzerland's ratification of the Convention on Cluster Munitions (known as the Oslo convention of 2010) in 2012, Switzerland has updated existing law banking involvement in War Materials including Nuclear, Biological and Chemical and extending this to the use, stockpiling, production and transfer of cluster munitions and anti-personnel mines because of their indiscriminate impact on civilian populations during and after armed conflict and bans direct and indirect financing of all these controversial weapons. UBS welcomed Switzerland's ratification of the Convention on Cluster Munitions. We announced at the time that we would be carefully analyzing the changes, which were to be made to Swiss law, and would amend our policies accordingly. Consequently, Swiss companies including Financial Institutions as well as their subsidiaries and affiliates anywhere in the world are not allowed to provide credit facilities, capital market transactions as well as buying and holding equity and/or bonds (including derivatives) of companies that are involved in the development, production or purchase of these controversial weapons. The revisions are likely to come into effect on 1st February, 2013.

2013 - Switzerland - Money Laundering Act - Proposed implementation of (a) FATF recommendations and (b) Financial Market Strategy⁷⁸

These proposals are a response to the FATF revised recommendations and provide that Swiss banks will in future have to refuse money from clients if they suspect that it has not been taxed, under proposals put forward by the government as part of measures to preserve the country's "integrity" as a financial centre. Also, people wanting to purchase real estate or luxury goods will not be able to pay more than CHF100,000 (US\$107,400) in cash, except through a regulated financial firm. Switzerland has proposed two new laws revising and updating existing laws on money laundering. The first takes account of new FATF requirements on combating money laundering and terrorist financing in the classic criminal sense. The second is to extend due diligence requirements to prevent untaxed assets from being accepted by financial intermediaries in Switzerland. For both proposals the consultation procedure is finished since 1 July 2013. The key points provided for in the proposed Law for implementing the FATF recommendations are the: Introduction of a disclosure obligation for holders of bearer and registered shares of

unlisted companies in order to enhance the transparency of legal entities, and the extension of the due diligence requirement for establishing the identity of beneficial owners, including identifying beneficial owners of operating companies above 25%; the duty to verify identity and risk-based due diligence requirements for politically exposed persons in Switzerland ("domestic" PEP's) and international organisations ("PEP's international Organisations"); and the introduction of a new predicate offence to money laundering in the form of qualified tax fraud in the area of direct taxation and an extension of the existing predicate offence in the area of indirect taxation. It was also proposed to move to an obligation to report suspicious transactions only (altering the existing dual right and obligation regime and removing therefore the right to report going forward). However, based on the input received in the course of the consultation procedure, the dual reporting system will be kept and the right to report will not be abolished. The proposal also changes the regime about blocking accounts. Once a SAR is filed the account is only blocked if the FIU sends the SAR for further investigation and as such notifies the Bank. It is thought that the Swiss may establish a threshold for tax fraud of CHF 200,000 illegitimate gains in order for this to qualify as a crime for money laundering purposes and would include the use of forged documents or deception of tax authorities for the purpose of tax evasion. Perhaps of particular interest is a new requirement targeting purchases of real estate and goods using cash, where these are to be prohibited if over CHF100,000, alternatively if larger these must be processed via a regulated financial intermediary. Finally, the effectiveness of the reporting system is to be increased and the procedures for financial firms to be simplified. In line with Switzerland's publicized intent on pursuing its financial market "Weissgeld" or "Whitemoney" strategy, a new proposed law requires regulated financial firms to operate a risk based approach to prevent the acceptance of untaxed assets, with indicators or red flags identified, for example: they can arise, from a client's wish for greater discretion or for investments to be carried out in an overly complex structure without any reasonable justification. The law likewise sets out indicators of situations where regulated financial firms can assume risks are reduced, for example if there is an international double taxation agreement between the client's country of domicile and Switzerland. Whilst the proposed new law does not mandate the use of a client self declaration a so called "Form T", where the Swiss Government has earlier announced that it was against introducing a widespread self declaration obligation, such an approach is still recognised as being capable of constituting a strong indicator of tax-compliant behaviour. The details are to be set out in self-regulation provisions that have to be recognised as a minimum standard by the supervisory authority. If the risk-based assessment reveals suspicions of a lack of tax compliance, regulated financial firms will have to refuse to accept assets in the future. If in the case of an existing client a change in behaviour, for

example, prompts justified suspicions that the client's assets are not tax-compliant, the regulated financial firm will have to ask the client to provide proof of tax compliance within a reasonable timeframe given the circumstances. If the client is unable to supply proof, the business relationship is ultimately to be terminated. The next phase is that the respective legal amendments will be submitted to the Swiss Parliament by the end of 2013. However, in the context of ongoing international initiatives and discussions, in particular on tax matters, further legislative action is unlikely, so that the so called Swiss Financial Market Place White Money Strategy will remain as a proposal until clarification and agreement is reached on the future of automatic exchange of information.

2013 - UN - The Arms Trade Treaty (ATT)⁷⁹
The ATT was adopted by the UN General Assembly in April 2013 and is part of a larger global effort begun in 2001 with the adoption of a non-legally binding programme of action at the UN Conference on the Illicit Trade in Small Arms and Light Weapons. This programme was formally called the "Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects" (PoA). The ATT establishes common international standards for the import, export and transfer of conventional arms. On behalf of the EU, Finland highlighted the support for the effort when it said, "everyday, everywhere, people are affected by the side effects of irresponsible arms transfers... As there is currently no comprehensive internationally binding instrument available to provide an agreed regulatory framework for this activity, the EU welcomes the growing support, in all parts of the world, for an ATT."

2013 - Singapore - Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act⁸⁰
As Singapore has grown into the world's fourth-biggest offshore financial centre, with more than US\$1.3 trillion in assets under management at the end of 2011 coming from overseas, and 50% growth in the five years to 2011, according to the latest government data, it has taken pre-emptive action to avoid criticism from other members of the OECD and implemented legislation and other measures to address new FATF requirements to include tax evasion as a predicate offence to money laundering. Starting from July 1, 2013, wilful and fraudulent tax evasion are included as serious tax crimes, and money laundering offences, which involve omissions, falsifications or fraudulent conduct perpetrated with wilful intent to evade tax or to assist others in evading tax. Before 1 July all financial institutions in Singapore must identify accounts they strongly suspect hold proceeds of fraudulent or wilful tax evasion and, where necessary, close them. After that, handling the proceeds of tax crimes will be a criminal offence. Still banks do not have to check that their clients are fully compliant with all their tax obligations, instead they must check if there are reasons to suspect the accounts contain the proceeds of serious tax offences

such as fraudulent or wilful tax evasion. As a result and in addition to scrubbing existing client files, banks will be expected going forward to develop and implement policies, controls and procedures to effectively detect and deter the laundering of proceeds from wilful or fraudulent tax evasion, to supplement existing client acceptance and ongoing transactions monitoring with tax-specific red flag indicators, as well as establishing proper escalation and investigation including Suspicious activity reporting procedures and educating and training employees. Both the Singapore Regulator the MAS and the recently issued Singapore Private Banking Code of Conduct for Client refers to possible red-flag indicators of tax crimes including: the use of complex structures or reliable negative tax-related reports on the client or on the client's jurisdiction of domicile or tax residence; the request and or use of holdmail services and or the non-collection over an extended period of hold mail without satisfactory reasons; non-face-to-face business relationships as well as other more generic AML red-flags such as suspicious and/or unusual or unexpected behaviour or activity.

2013 - BIS - Basel Committee on Banking Supervision - "Sound management of risks related to money laundering and financing of terrorism" - consultative document⁸¹

The BCBS has published updated advice on anti-money laundering (AML) and combating terrorist financing (CFT) best practice. The consultative document, released in June gives recommendations for AML/CFT risk management for banks, banking groups and supervisors. The BCBS suggests that recent "robust enforcement action" taken against a number of banks for AML failings "could probably have been avoided had the banks maintained effective risk-based policies". The Basel Committee has been offering advice on AML since 1988. The latest document provides updated recommendations for banks on how best to implement controls including for the first time details about the need for risk assessments, effective monitoring, good governance, strong IT systems and "three lines of defence" from staff in the front office, the chief AML officer and internal audits. The document goes on to assess problems that may arise for banking groups with cross-border operations. "Given the risks, each group should develop group-wide AML/CFT policies and procedures consistently applied and supervised across the group," the document says. This, the Basel Committee says, should include efforts to meet recommendations set out by the Financial Action Task Force, an intergovernmental AML body. In particular, banking groups should ensure "robust information sharing" between the head office and any branches and subsidiaries. However, such information sharing is not necessarily straightforward, as some jurisdictions restrict the sharing of customer information between the bank and group levels. In such cases, the Committee urged the jurisdictions to either change the rules, or ensure that banks were exempted.

Financial Action Task Force/FATF

FATF Work in 2013 (end Q2)



FATF issued in June 2013, the following 4 papers: 1) International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6); this paper provides best practices which will help countries in their

implementation of the targeted financial sanctions regimes to comply with the UN Security Council Resolutions (UNSCR) relating to the prevention and suppression of terrorism and terrorist financing; 2) Guidance on Politically Exposed Persons (Recommendations 12 and 22); the FATF has developed guidance which will assist in the effective implementation of AML/CFT measures to business relationships with Politically Exposed Persons (PEPs). Many PEPs hold positions that can be abused for the purpose of laundering illicit funds or other predicate offences; 3) Guidance: The Implementation of Financial Provisions of UN Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction; the FATF guidance assists countries in implementing not only targeted financial sanctions, but also other measures, such as activity-based financial prohibitions and vigilance measures; and 4) Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services; where New and innovative payment products and services are being developed and used at an ever-increasing pace, some have the potential of being used for money laundering or terrorist financing. This guidance examines how these payment products and services work, and how to develop and implement AML/CFT measures in line with the risk-based approach.

The FATF updated its lists of jurisdictions (i) with strategic anti-money laundering and combating the financing of terrorism (AML/CFT) deficiencies and (ii) Jurisdictions with strategic AML/CFT deficiencies for which they have developed an action plan with the FATF (see Part 1; Sub-section 4 Country Risk for details). Whilst there had been threats that Turkey would be suspended from its FATF membership following the October 2012 FATF meeting, Turkey was not in fact suspended due to

improvements made in the interim. For details see Part 1, Section 3, Sub-section 4 above.

FATF issued its Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems.¹ FATF have identified a High-Level Objective: Financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security and this is supported by 11 outcomes in order to identify and measure "Effectiveness". These include (i) Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation; (ii) International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets; (iii) Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks; (iv) Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions; (v) Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments; (vi) Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations; (vii) Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions; (viii) Proceeds and instrumentalities of crime are confiscated; (ix) Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions; (x) Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector; (xi) Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

For each outcome there are a choice of four ratings, (i) High Level of Effectiveness; (ii) Substantial Level of Effectiveness; (iii) Moderate Level of Effectiveness; (iv) Low Level of Effectiveness. Assessments should also make recommendations where appropriate in order to improve Effectiveness. First countries to be evaluated under the new system are Spain and Singapore.

FATF also updated the Guidance on Anti-Money Laundering and Counter Terrorist Financing Measures and Financial Inclusion² and approved and published guidance on conducting National Risk Assessment.

FATF also discussed the global challenges in supervision and enforcement. The plenary received and discussed presentations from US and UK representatives on the current state of compliance and of the supervision and enforcement of AML/CFT standards. Analyses of the experiences will be included in FATF's work on effectiveness. The FATF agreed to have regular discussions of this important issue.

FATF Work in 2012

In February, 2012 FATF issued their updated set of International standards on combatting money laundering and the financing of terrorism and proliferation with the release of the revised 40 Recommendations, with the most important changes being as follows:

a) **The Risk-based approach:** Countries need to clearly understand the money laundering and terrorist financing risks which affect them, and adapt their anti-money laundering/countering the financing of terrorism (AML/CFT) system to the nature of these risks – by applying enhanced measures where the risks are higher with the option of simplified measures where the risks are lower. The FATF has established the risk-based approach which will enable countries and financial intermediaries to target their resources more effectively. A well-implemented risk-based approach means that the AML/CFT system will be more effective, and will help countries implement measures to encourage financial inclusion, as called for by the G20.

b) **Transparency:** Lack of transparency about the ownership and control of legal persons and legal arrangements, or about the parties to wire transfers, makes those instruments vulnerable to misuse by criminals and terrorists. The FATF has strengthened transparency requirements in these areas. This means requiring that there is reliable information available about the beneficial ownership and control of companies, trusts, and other legal persons or legal arrangements. It also means more rigorous requirements on the information which must accompany wire transfers. Measures to improve transparency, implemented on a global basis, will make it harder for criminals and terrorists to conceal their activities.

c) **International Cooperation:** With the increasing globalisation of money laundering and terrorist financing threats, the FATF has also enhanced the scope

and application of international cooperation between authorities. The revised Recommendations will mean more effective exchanges of information for investigative, supervisory and prosecutorial purposes. This will also assist countries in tracing, freezing, and confiscating illegal assets.

d) **Operational Standards:** The FATF Recommendations concerned with law enforcement and Financial Intelligence Units have been expanded significantly. The revisions clarify the role and functions of the operational agencies responsible for combating money laundering and terrorist financing and set out the range of investigative techniques and powers which should be available to them, e.g., to obtain and analyse financial information about a suspected criminal's accounts and transactions

e) **New Threats & New Priorities:** The FATF is addressing new and aggravated threats and responding to the priorities set out by the international community, e.g. through the G20. The key issues addressed are:

- **Financing of Proliferation** - The proliferation of weapons of mass destruction is a significant security concern, and financial measures can be an effective way to combat this threat. The FATF has adopted a new Recommendation aimed at ensuring consistent and effective implementation of targeted financial sanctions when these are called for by the UN Security Council.

- **Corruption & Politically Exposed Persons** - The FATF Recommendations strengthen the requirements on financial institutions to identify politically exposed persons (PEPs) – who may represent a higher risk of corruption by virtue of the positions they hold. The existing requirement to apply enhanced due diligence to PEPs has been extended from foreign PEPs, with new risk-based requirements applied to domestic PEPs and PEPs from international organisations, and to the family and close associates of all PEPs – reflecting the methods used by corrupt officials and kleptocrats to launder the proceeds of corruption.

- **Tax Crimes** - The list of predicate offences for money laundering has been expanded to include serious tax crimes. This will bring the proceeds of tax crimes within the scope of the powers and authorities used to investigate money laundering. The smuggling offence has also been clarified to include offences relating to customs and excise duties and taxes. This will contribute to better coordination between law enforcement, border and tax authorities, and remove potential obstacles to international cooperation regarding tax crimes.

f) Terrorist Financing – The financing of terrorism remains a serious concern for the international community, and remains a major focus of the FATF Standards. The FATF's nine Special Recommendations on terrorist financing have been integrated fully within the Forty Recommendations, reflecting both the fact that terrorist financing is a long-standing concern, and the close connections between anti-money laundering measures and measures to counter the financing of terrorism.

g) Clarifying obligations: The FATF has updated its Recommendations to reflect practices in the financial sector (e.g., to set out clearer requirements for financial groups) and to apply the experience gained from the implementation of the FATF Recommendations by countries (e.g., by clarifying customer due-diligence requirements where countries have had practical difficulties with implementation).

International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations³

Note: *denotes the availability of Interpretative Notes.

A. AML/CFT POLICIES AND COORDINATION

1. Assessing risks and applying a risk-based approach*

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

2. National cooperation and coordination

Countries should have national AML/CFT policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies. Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence*

Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures *

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of bona fide third parties:

- (a) property laundered;
- (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences;
- (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, or
- (d) property of corresponding value.

Such measures should include the authority to:

- (a) identify, trace and evaluate property that is subject to confiscation;
- (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property;
- (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and
- (d) take any appropriate investigative measures.

Countries should consider adopting measures that allow

such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence*

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing*

Countries should implement targeted financial sanctions regimes to comply with UN Security Council Resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the UN Security Council under Chapter VII of the Charter of the UN, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation*

Countries should implement targeted financial sanctions to comply with UN Security Council Resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UN Security Council under Chapter VII of the Charter of the UN.

8. Non-profit organisations*

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are

particularly vulnerable, and countries should ensure that they cannot be misused:

- (a) by terrorist organisations posing as legitimate entities;
- (b) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and
- (c) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

D. PREVENTIVE MEASURES

9. Financial institution secrecy laws

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

CUSTOMER DUE DILIGENCE AND RECORD-KEEPING

10. Customer due diligence*

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence (CDD) measures when: (i) establishing business relations; (ii) carrying out occasional transactions:

- (i) above the applicable designated threshold (US\$/EUR 15,000); or
- (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
- (iii) there is a suspicion of money laundering or terrorist financing; or
- (iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means. The CDD measures to be taken are as follows:

- (a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
- (b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure

of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1. Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures. The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

12. Politically exposed persons*

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

- (a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- (b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
- (c) take reasonable measures to establish the source of wealth and source of funds; and
- (d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking*

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

- (a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
- (b) assess the respondent institution's AML/CFT controls;
- (c) obtain approval from senior management before establishing new correspondent relationships;
- (d) clearly understand the respective responsibilities of each institution; and
- (e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. Money or value transfer services*

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTs) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTs without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVT provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVT provider and its agents operate. Countries should take measures to ensure that MVT providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

15. New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to

- (a) the development of new products and new business practices, including new delivery mechanisms, and
- (b) the use of new or developing technologies for both

new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

16. Wire transfers*

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant UN Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

RELIANCE, CONTROLS AND FINANCIAL GROUPS

17. Reliance on third parties*

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

- (a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.
- (b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
- (c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for,

and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

18. Internal controls and foreign branches and subsidiaries*

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement groupwide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes. Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

19. Higher-risk countries*

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks. Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

REPORTING OF SUSPICIOUS TRANSACTIONS

20. Reporting of suspicious transactions*

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

- (a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred;
- (b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

22. DNFBPs: customer due diligence*

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

- (a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.
- (b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.
- (c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
- (d) Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client concerning the following activities:
 - buying and selling of real estate;
 - managing of client money, securities or other assets;
 - management of bank, savings or securities accounts;
 - organisation of contributions for the creation, operation or management of companies;

- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

(e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures*

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

- (a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.
- (b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
- (c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24. Transparency and beneficial ownership of legal persons*

Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements*

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES REGULATION AND SUPERVISION

26. Regulation and supervision of financial institutions *

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks. For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for

prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes. Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs*

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

(a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:

- casinos should be licensed;

- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and

- competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements.

This should be performed on a risk-sensitive basis. This may be performed by

(a) a supervisor or

(b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also

(a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a "fit and proper" test; and

(b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

OPERATIONAL AND LAW ENFORCEMENT

29. Financial intelligence units*

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities*

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of

crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers*

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system. Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed. Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4,

which would enable the confiscation of such currency or instruments.

GENERAL REQUIREMENTS

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

SANCTIONS

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

G. INTERNATIONAL COOPERATION

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the UN Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal as-

sistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

- (a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.
- (b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.
- (c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.
- (d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.
- (e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality. Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

- (a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and
- (b) a broad range of other powers and investigative tech-

niques; are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means.

Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation*

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering

and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations. In particular, countries should:

- (a) ensure money laundering and terrorist financing are extraditable offences;
- (b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;
- (c) not place unreasonable or unduly restrictive conditions on the execution of requests; and
- (d) ensure they have an adequate legal framework for extradition.

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation*

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts. Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.

FATF more work in 2012

FATF Public Statements naming and shaming Countries

Beyond the revision of the Recommendations, FATF made Public Statements first in June then updated in October about particular Countries that were effectively named and shamed, including naming North Korea and Iran where countermeasures were recommended and Turkey where FATF membership was proposed to be suspended. For more details about other Countries named see Part 2, Section 4, Country Risk above.

FATF Publications

In addition a number of other important announcements and publications were made.

FATF published its findings into the extent of **Money Laundering and Terrorist Financing vulnerabilities of the illicit tobacco trade⁴** at global, regional and domestic levels. According to FATF, the Illicit Tobacco Trade, which represents approximately one tenth of the global trade in cigarettes which is estimated at US\$40.5bio per year. In addition to its financial impact, illicit trade in tobacco also creates substantial loss of tax revenue. This FATF report analyses the extent of money laundering and terrorist financing vulnerabilities of the illicit tobacco trade at global, regional and domestic levels. The FATF also issued guidance in 2012 to help countries understand the important role of law enforcement in conducting money laundering, terrorist

financing and asset-tracing investigations. The guidance provides strategies and techniques which are intended to assist countries in increasing the effectiveness of such investigations. The Guidance is called “**Operational Issues - Financial Investigations Guidance**.” FATF also issued “**Specific Risk Factors in the Laundering of Proceeds of Corruption - Assistance to reporting institutions**”⁵ which was directed towards practitioners in the financial sector to better understand and identify the risk factors that may indicate the laundering of corruption proceeds.

Finally **G20 Finance Ministers and Central Bank Governors** reaffirmed their commitment to the FATF and issued a communique stating:⁶ “*We remain committed and encourage the FATF to continue to pursue all its objectives, and notably to continue to identify and monitor high-risk jurisdictions with strategic Anti-Money Laundering/Counter-Terrorist Financing (AML/CFT) deficiencies. We look forward to the completion in 2013 of the revision of the FATF assessment process. We encourage all countries to adapt their legal framework with a view to complying with the revised FATF’s Recommendations, in particular the necessity to identify the beneficial owner of corporate vehicles, and we look forward to the assessment of the effectiveness of the measures countries take and their compliance with the global standards in the next round of Mutual Evaluations.*”

FATF work in 2011

FATF issued 3 publications of real interest in 2011, the first, the “**Laundering the Proceeds of Corruption**”⁷ which studied the links between corruption and money laundering, key vulnerabilities within the current AML/CFT framework and some of the obstacles to the recovery of corruption; the second, “**Organised Maritime Piracy and Related Kidnapping for Ransom**”⁸ following on from a growing concern over organised piracy on the high seas and kidnapping for ransom; and finally “**Money Laundering Risks Arising from Trafficking of Human Beings and Smuggling of Migrants**”⁹ which describes the money flows related to trafficking of human beings and smuggling of migrants, and attempts to assess their scale.

FATF work in 2010

FATF issued 5 publications of real interest in 2010, the first, the “**Money Laundering Using Trust and Company Service Providers (TCSPs)**”¹⁰ was a comprehensive typologies report, then “**Money Laundering Using New Payment Methods**”¹¹ which compared the “potential risks” described in the 2006 report on New Payment Methods to the “actual risks” based on new case studies

and typologies, followed by a “**Global Money Laundering & Terrorist Financing Threat Assessment**”¹² aimed at raising the level of understanding of these threats and their negative impact, and helping governments to decide on what actions they can take; then “**Money Laundering through Money Remittance and Currency Exchange Providers**”¹³ which set out identified money laundering and terrorist financing methods and techniques involving money remittance and currency exchange providers; and finally, “**Money Laundering vulnerabilities of Free Trade Zones**”¹⁴ where concerns have been raised about illicit actors taking advantage of more relaxed oversight to launder the proceeds of crime and finance terrorism and the report highlights the vulnerabilities of free trade zones.

FATF work in 2009

FATF issued 3 publications of real interest in 2009 the first, “**Money Laundering and Terrorist Financing in the Securities Sector**”¹⁵ which studied (i) how criminals might be able to use securities firms to launder money and finance terrorism and (ii) how illicit funds can be generated through fraudulent activities; the second, “**Money Laundering through the Football Sector**”¹⁶ where several case examples of areas that could be exploited by those wanting to invest illegal money into football were described with concerns raised about the risks facing the football sector in particular and the sports industry in general to misuse by criminals; and finally “**Vulnerabilities of Casinos and Gaming Sector**”¹⁷ which included typologies and also considered vulnerabilities.

FATF issued a “Statement” on 25 February 2009 noting concerns and encouraging greater compliance by the following countries: Iran; Pakistan; Turkmenistan; Uzbekistan and São Tomé and Príncipe. For more details see Part 2, Section 4, Country Risk above.

FATF work in 2008

FATF issued 4 publications of real interest in 2008 the first a “**Typologies Report on Proliferation Financing**”¹⁸ the second, “**Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems**”¹⁹ then a “**Money Laundering & Terrorist Financing Risk Assessment Strategies**”²⁰ and a “**Terrorist Financing Typologies Report**”²¹.

FATF announced a successor programme to the NCCT programme which would be a different and more analytical process of identifying countries and jurisdictions displaying strategic deficiencies in their anti-money

laundering and anti-terrorist financing regimes,

FATF work in 2007

FATF issued 3 publications of real interest in 2007 the first, “**Money Laundering and Terrorist Financing Through the Real Estate Sector**”²² then “**Laundering the Proceeds of VAT Carousel Fraud Report**”²³ and “**The Misuse of Corporate Vehicles, Including Trust and Company Service Providers**”²⁴.

FATF’s final NCCT Review (Annual Review of Non-Cooperative Countries and Territories 2006–2007 dated 12 October 2007) listed no countries as non-cooperative.

FATF work in 2006

FATF issued 2 publications of real interest in 2006 the first a “**Report on New Payment Methods**”²⁵ and the second, “**Trade-Based Money Laundering**”²⁶.

The seventh NCCT list, published in June 2006, listed only Burma as non-cooperative.

FATF work in 2004

In 2004, FATF issued ‘**Combating the Abuse of Alternative Remittance Systems (SR VI) Best Practice, alternative remittance**’²⁷ which provided guidance on how to detect alternative remittance systems outside the conventional financial sector. FATF also issued ‘**Best Practice, cash couriers, bearer negotiable instruments, SR IX**’²⁸ which provided best practices for the areas that have proven most challenging.

FATF work in 2003

FATF issued its third revision of its 40/8 Recommendations.

FATF work in 2002

In 2002 FATF issued “**International Best Practices: Combating the Abuse of Non-Profit Organisations (SR VIII)**”²⁹ and “**Guidance for financial institutions in detecting terrorist financing**”³⁰ to help build awareness of how terrorists, their associates or those who support terrorism may use the financial system, this document describes the general characteristics of terrorist financing.

FATF work in 2001

In the second NCCT report issued in 2001 (including

a supplemental report later that year) a further eight countries were designated as non-cooperative: Egypt; Grenada; Guatemala; Hungary; Indonesia; Burma; Nigeria; and Ukraine. These would all ultimately be removed from the list over the coming years.³¹

FATF issued 8 Special Recommendations on Terrorist Financing.

FATF also issued a typology report on “**Behind the Corporate Veil**”.

FATF work in 2000

FATF introduced a blacklist which was published in June 2000, with fifteen countries initially appeared on the list as being regarded as uncooperative in the fight against money laundering. These included: Bahamas; Cayman Islands; Cook Islands; Dominica; Israel; Lebanon; Liechtenstein; Marshall Islands; Nauru; Niue; Panama; Philippines; Russian Federation; Saint Kitts and Nevis; and Saint Vincent and the Grenadines.³²

The FATF blacklist was the common shorthand description for the Financial Action Task Force list of “Non-Cooperative Countries or Territories” (NCCTs); that is, countries which it perceived to be non-cooperative in the global fight against money laundering and terrorist financing. The term “non-cooperative” was sometimes criticized as misleading, as a number of the countries which appeared on the list simply lacked the infrastructure or resources to cope with FATF requirements, and many considered them on the list for two main reasons. The first that they were not members of FATF and the second in that they were simply considered by some as having increased risks as so called offshore financial centres.

FATF work before 2000

1996 FATF makes its first revision of its 40 Recommendations and issues its first typology report.³³

1991 FATF members agree Mutual Assessment Process

1990 FATF issued its 40 Recommendations.³⁴

1989 FATF was established

Wolfsberg Group AML Standards & Work



In 1999 a group of international private banks,¹ with representatives from Transparency International, Professor Mark Pieth of the Basel Institute of Governance and the University of Basel and Stan Morris of Interpol, joined forces to review and compare their internal Anti-Money Laundering (AML) guidelines. The "Wolfsberg AML Principles for Private Banking," as they are now internationally known, emerged from this meeting. The name "Wolfsberg" was chosen as a brand name as a reference to the UBS Executive Development Centre at Wolfsberg, where the development meetings took place, as well as to the key role played by UBS in the establishment of this Group. The Wolfsberg Group is an association of 11 (initially 12) global banks, which aims to develop financial services industry standards, and related products, for Know Your Customer, AML and Counter Terrorist Financing policies. Current membership, besides UBS includes Banco Santander, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase and Société Générale.

By any measure the importance of the Wolfsberg Group cannot be understated. The Group is made up of 11 private sector banking groups, that are present in all continents and together have a presence in most of the countries of the world. The following facts and figures, collected from public sources and/or estimated by the author, also demonstrate the importance of the Group.

Whilst the total assets of the World's Top 100 Banks is estimated at almost US\$90 trillion and the total assets of the Wolfsberg Group combined are approximately US\$20.861 trillion, with 5 in the top 10 banks by asset, 9 in the top 20 and all 11 in the top 30.²

Total market capitalisation in aggregate for the members of the Wolfsberg Group as at end-April 2013 was just over US\$1 trillion (US\$1.015 trillion).³

In the major businesses that banks are involved, in particular; Asset Management; Brokerage; Commercial Banking; Correspondent Banking; Credit and Other Card Banking; Investment Banking; Retail Banking and

Wealth Management/Private Banking, Wolfsberg Group members are placed in many of the top places.⁴

It is estimated by the World Bank that 2.5 billion people do not have access to banking services. Of those that do, that is, approximately 5.5 billion, based on a global population of approximately 7 billion, it is estimated that the Wolfsberg Group members provide financial services to more than a billion of them.

The Wolfsberg Group members employ well over a million people, training all of their new and existing employees on the importance of money laundering prevention on a regular basis. Of these employees, thousands are solely dedicated to groups working directly on money laundering prevention issues, which together with investments in technology and run the bank costs supporting these tasks involves a direct financial cost to the Wolfsberg Group members of in excess of a billion dollars a year.

The work described below is not an exhaustive list of the Group's work, but are some of the more prominent papers and frequently asked questions (FAQs) issued by the Wolfsberg Group.⁵

The designations in the titles indicate how the Wolfsberg Group views the topic: 'Principles' are standards to be implemented by a financial institution throughout its operations, including branches and subsidiaries globally. 'Statements' on the other hand are position papers that delineate the role of financial institutions within a wider context. Guidelines and Papers are standards that are highly recommended but include optional approaches to the topic discussed. FAQs are chosen to explain a subject in more detail than would otherwise not be possible if another format was used.

The Anti-Money Laundering (AML) Principles 2000 / Global AML Guidelines for Private Banking 2002 (first revision)⁶

The first official and public piece of work by the Group focussed on money laundering in Private Banking. The work was completed following the exposure of numerous kleptocrats, most recently Sani Abacha of Nigeria and other so called "PEPs" including Raúl Salinas brother of Carlos Salinas, the ex-President of Mexico. This followed revelations against many former PEPs and would still be followed by those that would follow in their footsteps. The work started with a cooperation of internal standards and led to a compilation of best practices in Private Banking. The group would update their Standards later (see below). The AML principles, published in October 2000, were based on the more advanced AML laws and pre-empted those that would

soon afterwards be contained in the Basel Committee on Banking Supervision (BCBS) paper issued shortly afterwards. Principles included PEP and Beneficial Owner identification which was not the case in a number of countries at that time. The true novelty lay in the fact that the principles were to apply to all the banks' subsidiaries, including those in so called offshore centres and they contained the core elements of future work for the Group such as the Due Diligence Repository set out below, as well as detailed work on PEPs.

Statement Against Terrorist Financing 2002⁷

The terrorist attacks of September 11 2001 had a profound impact on the international financial sector and as such were of great concern to all the members of the Wolfsberg Group. The immediate reaction was the desire to play an active part in the fight against terrorism and at the same time to explain how financial institutions could help. The Group deliberated intensively over a short period of time and the Statement Against Terrorism Financing was issued in early 2002. The Statement demonstrated the Group's commitment in this area and identified areas of focus for both public and private sector to enhance success.

Correspondent Banking Principles 2002⁸

In fact, the second area of concern by the AML experts of the Wolfsberg Group was directed at Correspondent Banking, which, back in 2001, started to attract the attention of regulators and law enforcement. The Wolfsberg Group were the first to publish comprehensive recommendations on what, in their view, would be good practice in dealing with correspondents, and in particular when it comes to due diligence and monitoring.

Statement on Monitoring Screening and Searching 2003⁹

So far, the Group's work has stated the need for appropriate monitoring of transactions and customers to identify potentially unusual and suspicious activity and transactions, and for reporting such to competent authorities. However, it has not addressed issues related to the development of risk-based processes for monitoring, screening and searching of transactions and customers. The Group acknowledged that the risk profile may be different for a financial institution as a whole or for its individual units depending on the business conducted in a particular unit (for example, Retail, Private Banking, Correspondent Banking, and Broker Dealer). Any process is limited to detecting those clients and transactions that have identifiable characteristics that are distinguishable from apparently legitimate behaviours.

It becomes difficult, if not sometimes impossible, to make any distinctions between good and bad clients and acceptable and potentially illicit transactions because

money launderers and terrorists take all available actions to attempt to disguise their transactions and accounts by providing them with air of legitimacy. Three processes are defined: real-time screening, retroactive searching and transaction monitoring. The last process, monitoring, should not be limited to focusing of thresholds, but rather should be aimed at recognising unusual activity in comparison to known and expected activities.

Launch of the Bankers Almanac Due Diligence Registry 2004¹⁰

In the Wolfsberg Principles for Correspondent Banking issued in 2002, the Wolfsberg Group encouraged the development of an international registry for financial institutions which would enable them to obtain relevant information for due diligence on correspondent banks. The Wolfsberg Group started working on this topic with the Bankers' Almanac in 2003, and the latter then launched the "Due Diligence Repository" for the collection and storage of relevant due diligence information and documentation. The initiative aims to eliminate the need to reproduce, and repeatedly supply, due diligence information to counterparty banks. Instead, financial institutions can direct inquiries to the "Due Diligence Repository", where the most up to date due diligence information will always be stored. The Wolfsberg Group developed a list of required documents, reflecting recognised best practices with respect to necessary information to complete appropriate due diligence on which includes information on each financial institution's license (and the licenses of their subsidiaries), copies of corporate governance documents, biographies of board members and senior management, annual reports (including those of subsidiaries), and a completed, standard form Anti-Money Laundering Questionnaire.

During 2005 and early 2006, the Wolfsberg Group of banks actively worked on a number of separate papers, all of which aimed to provide guidance with regard to a number of areas of banking activity where standards had yet to be fully articulated by lawmakers or regulators. It was hoped that these papers would provide general assistance to industry participants and regulatory bodies when shaping their own policies and guidance, as well as making a valuable contribution to the fight against money laundering. These were:

Correspondent Banking FAQs 2006¹¹

The Correspondent Banking Principles were supplemented by FAQs published in 2006, which complemented the other sets of FAQs available on Beneficial Ownership, Politically Exposed Persons and Intermediaries.

Guidance for Mutual Funds and Other Pooled Investment Vehicles 2006¹²

The Group's work assists mutual funds and other pooled investment vehicles (e.g. unit investment trusts, hedge funds, private equity funds, and funds-of-funds) to manage their money laundering risk. Investors in many jurisdictions invest in these vehicles to seek professional management, diversification, and access to investment opportunities that might otherwise not be available. As a matter of general principle, there is no one approach to CDD that can be adopted by all pooled vehicles due to the variety of their characteristics and the different distribution channels. The appropriate level of CDD is determined on a combination of risks including investor, country, condition, and value. In a direct relationship, the vehicle should perform risk-based CDD on the investors. In an indirect relationship, the vehicle should consider the level of due diligence that should be performed in the intermediary taking into account the regulatory environment in the relevant jurisdiction, and the intermediary's responsibilities in respect of AML policies, procedures and controls. Depending on the outcome of the due diligence on the intermediary (and also on the requirement of applicable laws), the vehicle should determine the level of CDD on the investor.

Investment and Commercial Banking FAQs 2006¹³
Although much of the published guidance was also relevant to investment banking and commercial banking, certain aspects raising specific AML questions had not been addressed. They particularly related to questions on Financial Institution's clients in common scenarios, Customer Due Diligence (CDD) and its respective level in certain scenarios (when dealing with institutional intermediaries and their customers), or the Financial Institution's role in common and complex transactions. These FAQs also contain guidance that may be applied by Financial Institutions in the context of a reasonable risk-based approach to AML matters.

Guidance on a Risk Based Approach 2006¹⁴

At one of the first Wolfsberg meetings with regulators the idea of allocating resources in accordance with perceived risk was presented and discussed controversially among and within both the group of regulators and participating banks. After a few years the full merit of such a concept was acknowledged and accepted. In view of the wide practical implications of the introduction of such a concept, FATF invited Wolfsberg to nominate a representative to co-chair a joint working group to develop such a concept, which finally led to an FATF position paper and is now an integral part of the FATF 40 Recommendations. In parallel, Wolfsberg developed its own Statement, the Guidance on a Risk Based Approach for Managing Money Laundering Risks.

Statement against Corruption Guidance 2007¹⁵

The Statement against Corruption was issued in 2007. It focused primarily on corruption as a predicate offence to Money Laundering and was finalized in close association with Transparency International and the Basel Institute on Governance. It describes the role of the Wolfsberg Group and financial institutions more generally in support of international efforts to combat corruption. The Statement against Corruption identifies some of the measures financial institutions may consider in order to prevent corruption in their own operations and protect themselves against the misuse of their operations in relation to corruption.

Transparency of International Wire Transfers 2007¹⁶

Shortly thereafter, the Wolfsberg Group and The Clearing House Association LLC issued a statement endorsing measures to enhance the transparency of international wire transfers to promote the effectiveness of global anti-money laundering and anti-terrorist financing programmes. The four payment message standards that should be observed by all financial institutions are: (i) Financial institutions should not omit, delete, or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other financial institution in the payment process; (ii) Financial institutions should not use any particular payment message for the purpose of avoiding detection of information by any other financial institution in the payment process; (iii) Subject to applicable laws, financial institutions should cooperate fully as practicable with other financial institutions in the payment process when requesting to provide information about the parties involved; (iv) Financial institutions should strongly encourage their correspondent banks to observe these principles.

FAQs on PEPs revised and reissued 2008¹⁷

(the original FAQs, were issued in 2003)

PEP identification and risk management continue to be major issues for Financial Institutions and this update reflects the concept of the Risk-Based Approach which emerged as a major regulatory theme. The Group's focus has gone beyond private banking / wealth management and has addressed other financial services segments. Therefore, the Group's statements and principles have been viewed in a much wider context. There is no single, universally agreed definition of a PEP. In formulating these FAQs, consideration was given to the standards issued by internationally-recognised bodies such as the FATF. Local regulations may differ in respect of particular elements of the PEP definition, and should be considered by a financial institution when determining PEP categorization standards and relationship management procedures.

Statement on Monitoring, Screening & Searching revised and reissued 2009¹⁸

Developments and operational experience, for example in the use and relative effectiveness of dedicated, automated transaction monitoring systems, together with the introduction of the Risk Based Approach made it appropriate to revise the 2003 statement. It supersedes the former paper providing more guidance on the design, implementation and on-going maintenance of transaction monitoring frameworks for real-time screening, transaction monitoring and retroactive searches. The Group has committed itself to the development of appropriate standards and benchmarking for effective risk-based screening, monitoring and searching models. The type of monitoring framework implemented will depend on a financial institution's risk assessment and so will vary between institutions and even between business units with a financial services group.

Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities 2009¹⁹

Threats to, and vulnerabilities of, credit/charge cards "Issuing" activities in relation to money laundering initiated the Group's work which provides guidance on managing these risks as part of a comprehensive approach to AML compliance management. The paper also addresses merchant acquiring ("Acquiring") including the underwriting, provision and maintenance of point of sales relationships. Acquiring activities, and their attendant AML controls, may be closely aligned to the risks and controls associated with cards, any many large financial institutions extend services to both card and merchant customers. Whilst this guidance does not specifically address terrorist financing, the undertaking of appropriate customer identification, acceptance, initial and ongoing due diligence may assist in preventing terrorist and terrorist organisations from accessing all financial services, including those associated with the provision of credit card/charge card issuing and merchant acquiring.

Wolfsberg Anti-Corruption Guidance 2011²⁰

This Guidance superseded the earlier Statement, broadening the approach giving tailored advice to international financial institutions in support of their efforts to develop appropriate Anti-Corruption programmes, to combat and mitigate bribery risks associated with clients or transactions and also to prevent internal bribery. The Guidance was timely as it took into account a number of recent developments, notably new laws for example, the entry into force of the UK Bribery Act and the related Guidance issued by the UK Ministry of Justice. Both TI and the Basel Institute on Governance were involved in the final reviews of the paper

Trade Finance Principles 2009 and 2011²¹

Trade Finance, due to the high degree of technicality has been out of scope for most regulators or even compliance departments. With increasing worries about the abuse of trade finance for the purposes of money laundering, but also the proliferation of forbidden goods (Weapons of Mass Destruction), the Wolfsberg Group decided to ask its specialists to look into the matter and advise on whether general recommendations would be possible and useful to the industry. At the same time, FATF was taking an increased interest into the matter, however had to realize that on many aspects they lacked the technical expertise to make recommendations. To overcome this issue, the Wolfsberg Group advised, together with the International Chamber of Commerce, FATF on the more technical aspects. In the end, whilst FATF focused on more general recommendations, the Wolfsberg Trade Finance Principles are more concerned about practical aspects for financial institutions, but with reference to the more general FATF recommendations. The development of these respective documents is a good example of an independent but productive public private partnership.

Guidance on Prepaid and Stored Value Cards 2011²²

As part of the continuing development and use of what the FATF referred to as New Payment Methods in its Reports dated October 2006 and October 2010, it is recognised that there is a growing demand in the marketplace and in financial institutions for migration to electronic payments from paper based processes. It is also recognised that New Payment Methods are powerful tools in support of financial inclusion, which will result in further and more dynamic expansion of the market for products of this nature. The Prepaid Card is currently the most widely used of the available New Payment Methods. The broadening of the payment methods has resulted in greater complexity for regulators and for banks, in relation to assessing the risks attached to them and the application of, and responsibility for, AML controls, particularly if the transactions flow through one or more jurisdictions. An important aspect when considering New Payment Methods is that these products/applications are distributed by a much wider range of service providers, including non-bank service providers, than the more traditional paper based payment methods and the more traditional credit/charge cards. The segmentation of services between numerous and varied parties involved in the New Payment Methods add additional complexity. This paper was written with the collaboration of American Express, The Electronic Money Association, PayLife and Standard Bank South Africa.

Private Banking Principles 2012; FAQs on Intermediaries 2012 and FAQs on Beneficial Ownership 2012²³

Most recently in May 2012, the Wolfsberg Group announced that it has revised its Anti-Money Laundering Principles for Private Banking, together with the related FAQs on beneficial ownership and FAQs on Intermediaries/Authorised Signers. The Private Banking Principles were the first standards issued by the Wolfsberg Group back in 2000. The Principles were revised in 2002.

While the general thrust of the Principles remains the same, they have been clarified and updated to outline practices that had not been referenced before. In addition, in the interest of clarity, some language was repositioned from the FAQs to the Principles. The concepts related to beneficial ownership were further delineated. A new appendix has been added to the Principles that sets forth items that should be required from a due diligence standpoint.

In addition to work on standards and guidance for financial institutions an annual Conference is held, known as the Wolfsberg Forum.

The Wolfsberg Forum

The Wolfsberg Forum celebrated its 10th Anniversary in late May 2013, first held in 2004 and from the outset was regarded as an opportunity to bring together regulators, law enforcement and financial institutions from all over the world. Through such meetings the Group sought to discuss relevant topical issues in plenary and breakout sessions, to broach the possibility of future work products for the Group and to test possible approaches to emerging AML challenges. At the same time the Group opened its work to non-members for selected issues and thus secured a greater range of input from non-member banks. Examples of papers being developed in this way include the various card papers. Financial institutions invited to the forum are generally large, international financial institutions operating in major financial centres. The meetings are held in English with no translation facilities, they follow Chatham House rules and the Wolfsberg chairman opens the conference with a review of the previous year's developments and current challenges for the industry in the broad sphere of AML compliance. The Forum is regarded by many participants as the opportunity par excellence to speak openly to regulators and law enforcement as well as to peers, and presents an unparalleled opportunity to thrash out the theory of new or proposed policies against the realities of implementation. Unlike many conferences there are frank and open discussions with a limited number of set pieces and more time allocated to discussion in the plenary or in smaller workshops. The discussions and opinions aired at the forum are further

considered by the Group and may be used to inform their future work.

The 10th and most recent forum focussed on discussing a number of issues that are of particular importance including the drive for increased transparency but set against increasing concerns over the lack of privacy and increased data protection; the desire for greater financial inclusion whilst also accepting at the same time increasing exclusion of increased risk activities and an examination of the role of risk based approach and calls for greater prescription. Whilst these trends were examined, so were ideas and concerns over "effectiveness", "culture of compliance", "risk assessments" the future of "correspondent banking" and much more.

On the subject of correspondent banking the Group shared the latest draft of an updated paper on correspondent banking due for release shortly together with updated FAQs and an updated Due Diligence Questionnaire.

The Wolfsberg AML Risk Radar

During the 10th forum the Wolfsberg Group asked participants to risk rate areas of AML risk, covering (i) Predicate Offences; (ii) Customer Risks; (iii) Products and Services Risks; and (iv) Programme Component Risk that were of particular concern at this time.

The results make interesting reading.

Under i) Predicate Offences participants ranked the following in order of increasing importance: Tax, Bribery, Fraud, Terror Finance, Organised Crime, WMDPF, Drug Trafficking, Market Manipulation, Insider Dealing and Environmental Crime. Under ii) Customer Risks participants considered PEPs as presenting most risks followed by: MSBs, Intermediaries, Precious Metals and Stones Dealers, Banks and other financial institutions, Casinos and Internet Gambling Firms, Charities, Gatekeepers, Arms Dealers and High Value Goods Dealers.

For iii) Products and Services Risks were headed not surprisingly by Correspondent Banking and Wealth Management/Private Banking, followed by Commercial Banking, Asset Management, Brokerage, Cards, Retail Banking, and lastly Investment Banking.

For iv) Programme Component Risks Customer Due Diligence topped the list followed by Transaction Monitoring, Risk Assessment, Controls and Testing, Sanctions Screening, SAR Filings, AML Training and Investigations.

Sanctions & Embargoes



Economic sanctions are imposed by the UN and countries to address threats posed by the activities of governments, individuals and organisations. They can involve business restrictions and the freezing of property, and they can affect business

activities of all kinds. Sanctions restrictions might not always be considered a formal predicate offense to money laundering, but there are connections between sanctions and money laundering that can be useful if recognised.¹ Once persons are sanctioned and blocked from access to financial systems, they are forced to seek ways to travel, conduct business, transport materials and raise money without detection. For example, with charitable donations drying up as a result of sanctions, extremist groups turn to crime to generate funds, the proceeds of which must be laundered.

Moreover, some of the activities that sanctions target – terrorism, corruption, and trafficking in drugs, humans and arms – require the means to operate undetected. These activities flourish together in environments with ineffective regulatory schemes and give rise to collaboration among criminals. Successful transport routes for drugs can be transport routes for weapons, and a common interest in using these routes creates connections among networks. Al-Qaeda is believed to be financing its operations by exacting tolls from drug smugglers and traffickers in arms, humans and illicit goods. A network moving drugs from South America to Europe via West Africa was, according to US investigators,² supporting both Al-Qaeda and the Revolutionary Armed Forces of Colombia (FARC).³ US authorities sanctioned Lebanese Canadian Bank SAL for facilitation of money laundering by an international drug-trafficking network and funding of terrorist organisation Hezbollah.⁴

Finally, sanctions are sometimes imposed to prevent money laundering. An overlapping network of multilateral sanctions against senior officials in Libya, Tunisia, Egypt and Syria took form in early 2011 in response to the violent crackdowns aimed at the civil protests in the Middle East. A goal of these sanctions was to prevent the misappropriation of public funds by fleeing regimes.

As sanctioned persons become more adept at evading sanctions, financial institutions will be under even more pressure to improve their ability to see possible connections between suspicious activity and terrorist financing – whether they are examining trade finance transactions, companies with opaque ownership structures attempting to open accounts, or unusual transfers involving politically exposed persons.

Terrorism

Terrorism is a topic of concern for many countries that predates September 11. The UN has been working to combat international terrorism since 1972. Thirteen counter-terrorism international conventions are in force.

It has been challenging to define it. The UN adopted numerous international documents to identify specific acts of terrorism, such as acts against means of transport, hostage taking, certain substances or devices for terrorist purposes; financing and bombings. However, questions persisted. Does terrorism include acts of armed forces? What is the difference between a terrorist and a rebel or freedom fighter? Are Palestinians, Chechens, Kurds and Tamil Tigers terrorists or simply struggling for self determination?⁵

Another complicating factor in defining terrorism has been that terrorists have been commonly viewed as products of specific regional conflicts. Iran was named a terror supporter by the US primarily for its support of Hezbollah, an Islamic movement founded after the Israeli military seizure of Lebanon in 1982. Cuba was designated in 1982 by the US as a terrorism supporter for supporting Central American leftist revolutionary movements. The US imposed sanctions to stop Palestinian terror groups from fundraising in the US and in 1995 sanctioned persons threatening to disrupt the Middle East Peace Process. The NATO bombings in response to Milosevich 1990's 'reign of terror' was focused on the Balkans.

Nevertheless, the idea of a global terrorist threat took form by 1998. On 23 February 1998, bin Laden and associates announced an offensive global jihad to expel so-called Western interference from the Islamic lands' affairs, and called on Muslims to kill Americans and their allies in any country possible. In August 1998, simultaneous truck bomb explosions in US Embassies in Tanzania and Kenya killed hundreds. The US expanded existing sanctions programmes to include Al-Qaeda in 1998.⁶

UN Security Council Resolution 1267, adopted unanimously on 15 October 1999, established a sanctions regime to cover individuals and entities

associated with Al-Qaeda, bin Laden and/or the Taliban wherever located. It calls on Member states to freeze assets, deny entry or transit, and prevent arms from reaching listed individuals. The resolution acknowledged that activities, including fundraising, was occurring on a global level.⁷

9/11 - Attacks on America

September 11 attacks raised awareness of a global terrorist threat for a significant part of the world. On September 11, 2001, citizens of some 90 nations were killed when Al-Qaeda attacked the World Trade Centre in New York, and elsewhere, the US Pentagon and downed a flight enroute the Washington DC, demonstrating the threat that any part of the population could be victimized anywhere by groups waging ideological warfare. Subsequent terror attacks in locations such as Riyadh, London, Abuja, Madrid, Mumbai, and Kampala reinforced this view.⁸

A couple of weeks later, the UN adopted Resolution 1373, making it binding on Member States via Chapter VII of the UN Charter. The resolution requires States to criminalise terrorism and its financing, deny terrorists safe heavens and secure international borders. The resolution created a Counter-Terrorism Committee, all 15 members of the Security Council, charged with assisting with states' compliance with UN terrorism-related protocols and conventions. States send reports to the committee identifying their counterterrorism efforts in seven areas: legislation, financial asset controls, customs, immigration, extradition, law enforcement and arms traffic. UNSCR 1373 is viewed as a groundbreaking in that it gave the international community a new counterterrorism framework. Many states have revised existing or adopted new counterterrorism laws as a result. While UNSCR 1373 calls for States to freeze assets of terrorists, it does not provide a centralized list of sanctioned persons and entities and leaves States to determine for themselves who such persons and entities are.⁹

The UNSCR 1267 consolidated list (now known as the Al-Qaeda sanctions list) remains the UN list for terrorism designations and has been focused on Al-Qaeda and the Taliban. In 2011, the UN Security Council decided to split the Al-Qaeda and Taliban sanctions programmes. The sanctions list maintained by the Security Council Committee established pursuant to resolution 1267 will now be known as the "Al-Qaeda Sanctions List" and include only names of those individuals, groups, undertakings and entities associated with Al-Qaeda.¹⁰

Reforms

There was no right of appeal against a UNSCR 1267 listing until December 2006. On 19 December 2006, the Security Council voted to establish a de-listing procedure whereby those who found themselves on the list could petition the committee for it to consider their case.¹¹

Some governments have been reluctant to enforce sanctions against persons on the 1267 list, citing insufficient due process safeguards. In 2008 the European Court of Justice ruled the process violated human rights standards in *Kadi & Al Barakaat v. Council of the European Union and EC Commission*. The UN implemented reforms in 2009 to address criticism about the fairness of the sanctions list process. The UN Security Council voted unanimously to create an ombudsman to consider the removal of terrorist suspects from the 1267 list. Work began in early 2009 to review all names on the 1267 consolidated list by June 2010 and an ongoing annual review thereafter to ensure each designation is reviewed every three years. The reviews have resulted in several delistings.¹²

US Anti-Terrorism Programme

Post 9/11, the US began to see many more terrorist groups, regardless of their location or motivation, as a global threat, particularly given the ability for groups to act and raise funds on a global level. US President Bush issued Executive Order 13224, declaring that the acts of grave terrorism and the threats of terrorism committed by foreign terrorists posed an unusual and extraordinary threat to the national security, foreign policy, and economy of the US. Executive Order 13224 gave the US President the means by which to disrupt terror financing networks of all kinds by authorizing the US government to designate and block the assets of not only foreign terrorists, but those that provide material support or assist them. Groups previously designated as "foreign terrorist organisations" under pre-September 11 authorities were quickly re-designated under the new Executive order. The "national emergency" authorities targeting the Taliban were terminated, and Taliban names were designated under E.O. 13224. Colombia's FARC, the Sabotage Battalion of Chechen Martyrs, Sri Lanka's Liberation Tigers of Tamil Eelam have all been listed as SDGTs on the OFAC sanctions list.¹³

Shortly after 9/11, the US PATRIOT Act gave the US President authority to combat terrorism by designating persons for sanctions "in aid of investigation," meaning that OFAC could block assets of suspect entities prior to a formal designation to prevent the flight of assets and/or damaging behavior. The power has sparked US court challenges and claims that a person's property

could remain blocked for months or years without the person being formally designated. The US may avoid sanctioning US citizens with this power in the wake of a US court ruling that OFAC blockings are "seizures" within the US Constitution's Fourth Amendment and therefore require due process protections.¹⁴

The differences between the US sanctions programmes and those of other authorities become more visible when institutions are attempting to comply with multilateral sanctions. An example is the fact that the US may block property not actually owned by a sanctioned party. The term "interest" is broadly defined in OFAC's sanctions regulations in Chapter V of Title 31 of the Code of Federal Regulations. An interest in property may be direct or indirect and includes property interests short of full ownership. In many instances, the interest may be partial or contingent. Therefore, innocent third party's funds could be stopped by a financial institution and frozen indefinitely because of a connection to a sanctioned party.¹⁵ The US annual Terrorist Asset Report published for the US Congress may list assets not actually belonging to terrorists. In its annual 2010 Terrorist Assets Report, the US Department of the Treasury explains:

Because the blocked assets discussed in this report include assets not actually owned by designated or blocked parties, they are described throughout as assets "relating to" a designated party. Many of the assets may be owned or subject to claims by third parties. This has created ownership disputes in US courts between holders of terrorism related judgments attempting to attach blocked assets and those persons whose property has been blocked by US financial institutions.¹⁶

In contrast, there is little formal guidance indicating that other nations enforce terrorism sanctions to this degree. UN resolutions call for Member States to freeze without delay the funds and other financial assets or economic resources "of" designated individuals and entities, implying a property interest.¹⁷

In August 2012, the US Government passed the Iran Threat Reduction and Syria Human Rights Act ("ITRA") which strengthened sanctions targeting Iran including those under the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ("CISADA"). The act also targeted human rights abuses in both Iran and Syria. In sum, the ITRA substantially broadened the activities sanctionable particularly those relating to the providing services to Iranian government-linked entities, UN and US sanctioned persons, affiliates of Iran's Revolutionary Guard Corps, expanded

sanctions against Iran's energy sector, among other sanctions.¹⁸

Notably, ITRA also added a new section under the Securities Exchange Act of 1934 to require any US issuer to report in its annual public SEC filing whether the issuer or its affiliates (including non-US affiliates) had knowingly engaged in any Iran-related activities, or involved persons or entities designated as weapons of mass destruction proliferators or terrorists. The SEC is then required to report to the US President who is mandated to investigate and make sanctions determination.¹⁹

9/11 Litigation Cases

Thousands of civil suits have been filed by a variety of plaintiffs claiming negligence or other harm as the result of or following the attacks on 11 September 2001. For example, plaintiff's have claimed that airlines were negligent in permitting the 9-11 terrorists to board the aircrafts carrying items that could be used as weapons;²⁰ other suits have related to litigation filed by first responders (relating to, for example, inoperable radios on the day of the attacks), and sanitation workers (relating to health problems after being exposed to debris at "ground zero" or at the landfill on Staten Island where much of the debris, including human remains, were transferred from the Trade Centres).²¹ Countless businesses and insurance companies have battled over coverage for billions of dollars in property damage and lost property income.²² Suits filed by thousands of plaintiffs, including firms like Cantor Fitzgerald, a firm which lost 658 employees, and the 9/11 Families United To Bankrupt Terrorism, comprised of more than 6,600 family members of those killed in the attacks, have been based on claims that charities and countries like Saudi Arabia were complicit in financing the terrorists.²³ Still other suits have related to who gets the deposits of home buyers who withdrew from real estate deals following the tragedy. Litigation has even involved law suits filed before the 9-11 attacks due to lost documentation and evidence destroyed in the attacks.

Most of the victim's families have chosen to apply for payments under the Victims Compensation Fund which was established by the US Congress to assist those directly impacted by the attacks, rather than face the risks in filing a lawsuit.²⁴ However, other families angry at the failures in security have pursued litigation to seek answers rather than for financial recovery. Even more emotional have been the cases pitting family members against family members as to where to bury remains of victims. While many lawsuits have been settled by the parties or decided by judges, hundreds of other cases will likely continue for years to come.

Notably, a 2009 decision by the US Supreme Court will allow judges to dismiss a case if at the outset there are no concrete facts to state a plausible claim for relief. In the past, a plaintiff simply had to submit short bare-bones complaint to force a defendant to open their files and answers questions as part of the discovery process at great cost to the defendant. In *Ashcroft v. Iqbal*, the court ruled that a Muslim man could not sue two Bush administration officials for abuses he alleged he had suffered after being detained following the attacks.²⁵

Drug Trafficking

The US administers two list-based sanctions programmes aimed at narcotics trafficking.²⁶ The first is a programme that focuses on the Colombian cartels, and the second targets narcotics kingpins globally.²⁷ Both programmes were designed with the view that trafficking requires supporting networks, and each programme can sanction individuals and entities for assisting narcotics traffickers or for being owned or controlled by them.

Cali Executive Order 12978

In 1995, the US used the list-based approach of terrorism Executive Order 12947 as a model for a new programme to target Colombian drug cartels.²⁸ With Executive Order 12978, the President identified four Cali Cartel drug kingpins and expanded the order into a key tool in the fight against the Colombian Cartels. Entities and individuals associated with the Cali, North Valle, and North Coast Cartels and their business empires have been designated as Specially Designated Narcotics Traffickers ("SDNTs") under the order.²⁹

Building on the successes of the Colombian cartels programme, in 1999, the US Congress enacted the Foreign Narcotics Kingpin Designation Act ("Kingpin Act"). The Kingpin Act provides a statutory framework for sanctions against foreign drug kingpins and their organisations on a global scale. Like the terrorism programme under Executive Order 12947 and the SDNT programme under Executive Order 12978, the Kingpin Act is directed against the individual or entity and their support infrastructure, not against the countries in which they are located. Foreign persons designated under the Kingpin Act are referred to as "[SDNTK]s" on OFAC's listing of "Specially Designated Nationals and Blocked Persons" to differentiate them from the Specially Designated Narcotics Traffickers [SDNTs] named under Executive Order 12978. The Kingpin Act has its own set of civil and criminal penalties.³⁰ Over 1,000 individuals and entities have been designated for sanctions under the Act.

The targeting of individuals with asset freezes was seen by many as an effective alternative to the "War on Drugs" originally declared by US President Nixon in the 1970s, which was sometimes criticised as a cover for covert military operations to fight leftist insurgencies in Latin America. A 1986 US programme to deny aid to countries not "certified" as cooperating with the US War on Drugs was also largely viewed as counterproductive.³¹ The US has cited as one example of the list-based approach's success the guilty pleas of two Colombian kingpins in 2006 to make their families eligible to be removed from OFAC's designation list.³²

Over the past several years, the US has sanctioned nearly 3000 entities in Latin America involved in narcotics trafficking – almost 1800 entities have been designated under Executive Order 12978, and nearly 1,000 entities have been sanctioned pursuant to the Foreign Narcotics Kingpin Designation Act (the "Kingpin Act"),³³ (taken from June 24, 2011, OFAC Testimony Before the Oversight and Government Reform Subcommittee on National Security, Homeland Defence, and Foreign Operations, the Foreign Affairs Subcommittee on the Western Hemisphere, and the Foreign Affairs Subcommittee on the Middle East and South Asia). Though relatively few, the majority of delistings involve narcotics sanctions programmes designations. This makes sense, given that so many of the narcotics trafficking programme designations are based on commercial connections to networks attempting to launder drug money. Delistings can occur if (1) there is an insufficient basis for the designation (for example, error) or (2) the original reasons for the designation no longer exist (for example, resignation from a position with a sanctioned corporation or evidence of a corporate reorganisation that would eliminate control of an SDN).³⁴

Weapons of Mass Destruction

Weapons of Mass Destruction (WMD) are generally defined as weapons designed for mass, indiscriminate destruction, to kill large numbers of civilians and military personnel. The types of weapons considered to be in this class include: Nuclear weapons (including radiological weapons); Biological weapons; Chemical weapons; and Explosive material; as per UN Resolution 1540.³⁵

In 2004, the UN Security Council sought to limit the acquisition of WMDs by terrorists. Post 9/11, concerns centred on terrorist and black market networks obtaining WMD and related components, particularly from ex-soviet countries without effective export controls. The Council adopted Resolution 1540 establishing for the first time binding obligations on

all UN member states under Chapter VII of the UN Charter to take measures against the proliferation of WMD. The Resolution doesn't impose sanctions, but requires states to: (1) adopt and enforce laws prohibiting the proliferation of such items to non-state actors, and prohibiting assisting or financing such proliferation; and (2) take and enforce effective measures to control these items, in order to prevent their proliferation, as well as to control the provision of funds and services that contribute to proliferation.³⁶ The resolution followed public revelations about a North Korean nuclear weapons programme in October 2002 and revelations about Iran's nuclear programme in May 2003, two countries designated by the US as terrorism supporting states.³⁷

In addition to imposing WMD-related sanctions against countries like Iran and North Korea, the US imposes list-based sanctions against individuals and entities involved in WMD proliferation. OFAC implements three distinct sanctions programmes designed to combat the proliferation of WMD.

The first and earliest is an import ban. OFAC's Weapons of Mass Destruction Trade Control Regulations, 31 C.F.R. Part 539, implement a ban on imports into the US, pursuant to Executive Order 12938, of 14 November 1994. Under this programme, the Secretary of State may name, as subject to the ban, foreign persons determined to have engaged in proliferation related activities. 24 individuals and entities remain subject to these restrictions.³⁸

This programme was later enhanced with a blocking programme. Executive Order 13382 of 28 June 2005, requires US persons to block the property of individuals and entities engaged in proliferation activities and their support networks. It was created to take additional steps with respect to the Executive Order 12938. OFAC administers this blocking programme, which initially applied to eight organisations in North Korea, Iran, and Syria. To date, companies from over 25 different countries have been sanctioned under Executive Order. Most of the designations concern Iran, including Iran's biggest banks.³⁹

There is a third US programme regarding WMD that involves the US Government's use of sanctions to prevent judgment creditors from interfering with a uranium exchange between the US and Russia. A 1993 deal involved Russia's sale of highly enriched uranium extracted from dismantled Russian nuclear weapons to the US for conversion for use in commercial reactors. Uranium shipments were halted in 2000 because of US legal proceedings concerning a Swiss company's claim

against the Government of the Russian Federation that could have resulted in a judgment against payments owed by US to Russia or against processed uranium deliveries.⁴⁰ As a result of this delay, the President issued an Executive Order on 21 June 2000 that blocked the Russian Government's assets directly related to the implementation of the agreement from any judgment, thus allowing the shipments to resume.⁴¹

Country Sanction Programmes

The following are brief summaries of Sanctions issued by one or more important Bodies.

Belarus

In December 2010, tens of thousands of Belarusians arrived at a square in Minsk to protest President Alexander Lukashenko's re-election victory, reportedly with 80% of the vote. Lukashenko responded with a violent crackdown. Belarusian riot police beat and arrested over 600 protesters, including most of the opposition candidates and many journalists and human rights activists.¹ Following the demonstrations, the Government raided offices and pursued opposition party members and the press. Opposition leaders were sentenced to prison for organising the protests. The EU and US responded by expanding existing sanctions against the Lukashenko regime.²

Lukashenko, often referred to as "Europe's Last Dictator," has been in power since 1994 as a result of elections that international observers describe as rigged. He has repeatedly used brutal force against opposition demonstrators. After ten years in power, he changed the constitution, using a manipulated referendum, to allow himself to serve a limitless number of consecutive presidential terms. Reports from the UN, US and European organisations have cited Belarus' disregard for human rights, corruption and use of the judiciary for improper political ends.³

The EU has applied targeted sanctions for years against Belarusian government representatives including electoral commission heads, ministers, security service officers, prosecutors and judges. In 2004, the EU issued travel bans against four individuals believed responsible for the disappearance of opposition members.⁴ The EU expanded this travel ban in 2006 to an additional 36 persons responsible for committing election fraud, and introduced an asset freeze. In the autumn of 2008, it suspended the travel ban against 36 people, in response to Lukashenko's release of opposition representatives from prison.⁵ Following the December 2010 election crackdowns, the EU restrictions reinstated the travel ban against Lukashenko and associates, and introduced additional asset freezes and an embargo on arms and

equipment that might be used for internal repression.

The US, acting with the EU, imposed in 2006 travel restrictions and targeted financial sanctions against Belarusian officials implicated in the human rights abuses and election fraud.⁶ In 2007, the US extended travel restrictions to directors and deputy directors of state enterprises and froze the US assets of Belarus' oil and chemical conglomerate, Belneftekhim.⁷ After the Belarusian authorities released the last of its political prisoners in 2008, the US suspended sanctions for 6 months on two Belneftekhim subsidiaries, Lakokraska and Polotsk Steklovolokno. In 2011, however, the US reinstated these sanctions and blocked four more Belneftekhim subsidiaries. Beginning in 2006, Switzerland also joined the EU in targeting Belarusian officials for sanctions.⁸

Media sources report that Belarus is beginning to act as middleman for Iran's access to Russian technology. Its role is reported as key to Iran's development of surface-to-surface missile and nuclear capabilities, particularly given the drastic reduction in Iran's ability to procure products from countries such as China, Russia and Dubai. In 2009, Belarus was reported to be selling Russian-made Iskander-M tactical missile systems⁹ to Iran, which the Belarus government has denied. In March of 2011, the US imposed sanctions on, Belarusneft, a state-owned energy company in Belarus for its involvement in the Iranian petroleum sector.¹⁰

Democratic Republic of the Congo

A multilateral arms embargo is in place, and an asset freeze targets political and military leaders responsible for armed conflict and human rights violations in the Democratic Republic of the Congo.¹¹ However, no broad-based sanctions restrictions are in effect against the people or the country of the DRC.

The Democratic Republic of the Congo is a large country that shares borders with nine other countries, and has been devastated by political violence. The government does not have control over the large parts of its territory, particularly in the east where armed groups continue to fight and where the prevalence of rape and other sexual violence is the worst in the world. President Joseph Kabila does not maintain central control over the country's military. The provinces where metal mining takes place are overrun with militias and rogue army units that finance themselves with the region's metal mining. These conditions are remnants of two wars on DRC soil involving several African countries.¹²

The First Congo War (1996). In the wake of the 1994 Rwandan genocide, in which 800,000 Tutsis

and moderate Hutus were killed, millions of Rwandan refugees flooded into the eastern DRC. Although UN sources estimated that only a fraction of these refugees acted in the genocide, Rwanda and Uganda invaded eastern DRC in 1996 to root out genocide perpetrators, teaming with Congolese opposition leader Laurent Desiré Kabila. This force defeated DRC dictator Mobutu Sese Seko and the Congolese army, and Laurent Desiré Kabila became President.

The Second Congo War (1998) involved seven foreign armies and killed over 5.4 million people. It began when President Laurent Kabila ordered Rwandan and Ugandan forces to leave the eastern DRC, fearing they would try to annex the mineral-rich territory. Rwanda had ties to the Tutsi community in eastern DRC and feared for its safety. Angola, Zimbabwe, Chad, Libya and Sudan supported Kabila in this conflict against Uganda and Rwanda. Despite a 1999 ceasefire and peace agreements signed in 2002 and 2008, multiple armed groups continue to destabilize the region and terrorize civilians. Tutsi forces have pursued the Democratic Forces for the Liberation of Rwanda (FDLR), which is led by persons held responsible for the Rwanda genocide.¹³

On 28 July 2003 the UN Security Council (UNSC) adopted resolution 1493 (2003) imposing sanctions in relation to the DRC in response to acts of violence systematically perpetrated against civilians, including massacres, other atrocities and violations of international humanitarian law and human rights.¹⁴ The sanctions regime was modified and strengthened with the adoption of resolutions 1533¹⁵ (2004), 1596 (2005), 1649 (2005), 1698 (2006), 1768 (2007), 1771 (2007), 1799 (2008) and 1807 (2008).¹⁶

All States remain under an advance notification obligation regarding any shipment of arms and related materiel for the DRC. The UNSC further extended the arms embargo and targeted travel and financial sanctions in resolution 1952 (2010) against FDLR leaders and a former Congrès National pour la Défense du Peuple commander integrated in the Congolese Armed Forces.¹⁷ Authorities including EU, Australia, Switzerland, Canada, US, Singapore and Hong Kong have implemented restrictions based, in whole or in part, on UN resolutions.¹⁸ Additionally, US requires companies to disclose the exact source of metals procured from the Congo.

President Laurent Kabila was assassinated in 2001 and his son Joseph Kabila was appointed and in 2006 won the presidency in the DRC's first democratic elections in 40 years.¹⁹

Cuba

The US economic embargo against Cuba remains comprehensive, targeting both the Cuban Government and Cuban nationals. It prohibits trade, payments and financial services with limited exceptions, and it requires the freezing or blocking of property in which Cuba or Cuban nationals have an interest. This is the oldest US trade embargo, but the US regularly conducts cash trade with Cuba via licenses for the sale of food and medical supplies.

The Cuba embargo has existed since the 1960s, when it was created from broad presidential powers to address war time threats. A trade embargo was imposed in 1960 after Cuba nationalized property of US citizens and companies. In 1963, the US froze Cuban assets in the US and imposed a complete embargo against Cuba and its citizens in response to the Cuban Missile Crisis, during which Cubans hosted Soviet nuclear weapons approximately 90 miles from the US mainland.²⁰

The embargo was tightened in 1996 by the Cuban Liberty and Democracy Solidarity Act (known as the Helms-Burton Act) after Cuban fighter jets shot down two planes piloted by a Cuban exile group off the Cuban coast. The law permits lawsuits in American courts against non-US companies who invest in businesses once owned by Americans or by Cubans now living in the US. In response to the Helms Burton Act, Canada, Mexico, the EU and the UK created measures to counteract the extraterritorial effect of the Helms Burton Act.²¹

The US continues to view Cuba as a State Sponsor of Terrorism, particularly for its provision of physical safe haven and ideological support to members of - the FARC, ELN, and ETA providing them with living, logistical, and medical support. The US has designated the three organisations as Foreign Terrorist Organisations.²²

Nevertheless, the US loosened restrictions in 2011 with licenses for transactions with Cuban nationals residing outside of Cuba, travel for educational and religious activities, family remittances and payments to support of religious activities.²³

Palestinian Territories

Currently, the Palestinian Authority is sanctioned by the US only in so far as its activities involve an interest of Hamas. However, several banks processing transfers involving the Palestinian territories have found themselves the targets of civil litigation.²⁴

The 2006 parliamentary elections in the West Bank

and Gaza resulted in members of the terrorist group Hamas forming the majority party within the Palestinian Legislative Council and holding positions of authority within the government. In response, the US government determined that Hamas had a property interest in the transactions of the Palestinian Authority. This determination meant that US persons could not engage in transactions with the Palestinian Authority unless authorized by the US. However, dealings with private companies and individuals in the Palestinian Territory were permitted, as were dealings with local government not part of the Palestinian Authority.²⁵

In 2007, Salam Fayyad became the new Prime Minister of the Palestinian Authority and appointed as ministers other individuals not affiliated with Hamas. OFAC issued a license that essentially lifted the sanctions against the Palestinian Authority created by OFAC's earlier guidance. OFAC defined the Palestinian Authority as the government of Prime Minister Salam Fayyad and President Mahmoud Abbas, including all branches, ministries, offices, and agencies.²⁶

Despite the license, it has not always been easy to distinguish between transactions destined for the West Bank and Gaza that ultimately benefit Hamas and those that do not. The Palestinian Authority has not been able to combat terrorism in the West Bank because of limited mandates and because of Hamas' continued control. The US government reports that in 2010 an organised Hamas force of 15,000 continued to consolidate control over Gaza by marginalizing rivals. Gaza-based Palestinian terror groups staged rocket and mortar attacks into Israeli territory and over 100 terrorist incidents were reported as taking place in 2010 near Gaza's security perimeter. Groups involved included Hamas, the Palestinian Islamic Jihad and the Popular Resistance Committee. Rockets with larger warheads and longer ranges are being built within Gaza. Iran is providing medium range rockets. Israel enforces strong measures to restrict economic activity with Hamas controlled Gaza Strip.²⁷

Several banks face multimillion dollar civil law suits brought in the US by terror victims alleging that the banks processed transactions involving Hamas. Below are some brief examples:

Linde v. Arab Bank

In 2004 three groups of Israeli based plaintiffs alleged they or their family members were harmed by acts of terrorism that occurred in Israel or the West Bank/Gaza from 1995 to 2005. They allege that the bank held accounts for individuals and organisations that, in turn, supported terrorist activities. Plaintiffs specifically argue

that the bank is liable for processing payments sent by the “Saudi Committee in Support of the Intifada Al Quds” to Palestinians from 2000 through 2004. These payments, according to the plaintiffs, were intended to encourage acts of terrorism.

The bank maintains that it provided routine financial services in compliance with governing laws and regulations. It denies ever knowingly supporting terrorism in any way. According to the bank, the Committee was not an account-holder, it believed that the Committee was a legitimate humanitarian organisation, and its role in handling the Committee payments was limited to processing transfer instructions sent from a correspondent bank in Saudi Arabia.

To date the Committee has not been designated as a financier of terrorism by the US.

In 2007, the bank filed third-party complaints against Bank Hapoalim, B.M., Israel Discount Bank Ltd. and Mercantile Discount Bank Ltd., alleging that each of these banks initiated or processed funds transfers for some of the same organisations that plaintiffs allege served as well known “fronts” for terrorist organisations. The bank argued that to the extent that it might be found liable to plaintiffs for providing financial services to these same organisations, Bank Hapoalim, B.M., Israel Discount Bank Ltd. and Mercantile Discount Bank Ltd. should contribute to any damages.²⁸

On 3 April 2009, the District Court dismissed the claims against Bank Hapoalim, B.M., Israel Discount Bank Ltd. and Mercantile Discount Bank Ltd. after finding that neither the Anti-Terrorism Act nor the Alien Tort Statute provided the bank with a right to seek contribution from parties that were not named in plaintiffs’ complaints. The bank previously sought discovery from Bank Hapoalim, B.M. and Israel Discount Bank Ltd. arguing that those Israeli banks initiated or participated in financial transfers for some of the same parties that plaintiffs allege were well-known “fronts” for terrorist organisations that directed their violent activities against the State of Israel. The bank argued that these records, if produced, would offer “circumstantial evidence of [its] lack of knowledge” that the charities at issue were allegedly well-known “fronts” for terrorist organisations opposed by Israel. However, the Bank’s discovery requests as to Israeli bank records were denied after the Court, via Judge Gerhson, found that those records were protected from disclosure by foreign financial privacy laws.²⁹

In November 2010, Arab Bank filed for a Writ of Mandamus against Judge Gerhson, alleging that she had abused

her discretion by overriding the recommendations of her magistrate and by imposing such severe sanctions without further hearings. In addition Arab Bank’s lawyers asserted that Gerhson failed to duly respect the secrecy laws regulating the bank in Jordan, Lebanon and the Palestinian territories. Significantly, the Jordanian government submitted an amicus curiae in support of Arab Bank, also asserting that any damage to the bank had the potential to undermine global anti-terrorism prospects by forcing customers into underground financial systems that would be much harder to monitor. Further support was lent by amicus curiae briefs submitted by the Union of Arab Banks and the Institute of International Bankers. The petition for a Writ of Mandamus was heard on 6 March 2012 by three judges of the Second Circuit.

On 18 January 2013 the Second Circuit dismissed Arab Bank’s appeal and denied its petition for a writ of mandamus, on procedural grounds, stating that it didn’t have jurisdiction to hear the appeal pre-trial. In its decision, the court said, “the sanctions order is not a reviewable collateral order, and we therefore dismiss the bank’s appeal for want of jurisdiction.” On 14 February 2013, the bank filed a letter with the Second Circuit submitting as supplemental authority the Second Circuit’s decision to uphold a lower court’s dismissal of Rothstein v UBS.

Rothstein v. UBS

In Rothstein, a case which was brought against UBS by 45 victims of terrorist bombings and rocket attacks in Israel by Hamas and Hezbollah between 1997 and 2006, the Plaintiffs claimed that while UBS did not have direct dealing with the terror groups, cash exchanges made by the bank pursuant to an Extended Custodial Inventory Agreement with the Federal Reserve subjected it to OFAC regulations. The plaintiffs argued that the bank’s actions had aided and abetted international terrorism in violations of those sanctions and therefore, under the Anti-Terrorism Act of 1990 (ATA), was subject to civil liability to victims of these terror attacks. The court held that the plaintiffs had failed to establish UBS’ actions were a “proximate cause” of the terrorist acts committed by Hezbollah and Hamas and funded by Iran and therefore, under ATA, Plaintiffs were not entitled to recovery.

Weiss v. National Westminster Bank

Terrorism victims and their families have sued National Westminster Bank, or NatWest, which is part of the Royal Bank of Scotland Group, for maintaining accounts of the Palestinian Relief and Development Fund, a British charity known as Interpal. The Israeli Government designated Interpal as a terrorist organisation in 1998, and the US designated Interpal as a Hamas fund-raiser in 2003. Plaintiffs in the case

include relatives of victims of a Hamas suicide bomber on a bus in Jerusalem on 19 August 2003. NatWest responded in legal papers that UK charity regulators had twice cleared Interpal of terrorist links. The court initially refused to grant the bank’s motion to dismiss.³⁰ On 28 March 2013 the Court granted summary judgment to NatWest finding that the plaintiffs had failed to establish sufficient evidence to prove that NatWest either “had actual knowledge” that Interpal was funding Hamas or had acted with “exhibited deliberate indifference”. In assessing the banks state of mind, the Judge noted the banks compliance with foreign banking laws. This decision has been appealed.

Strauss v. Crédit Lyonnais

Crédit Lyonnais is a defendant in a civil suit alleging that the institution held accounts for French charity CBS. The suit is brought by family members of victims of terrorist attacks occurring between March 28, 2001 to August 19, 2003. The US designated CBS in 2003 for fundraising for Hamas in collaboration with humanitarian organisations in the West Bank, Gaza, Jordan and Lebanon. The State of Israel outlawed CBS in 1997, and designated it a terrorist organisation in 1998. Crédit Lyonnais maintained accounts for CBS and transferred funds at CBS’s request to Hamas-controlled organisations in the West Bank and Gaza Strip. The plaintiffs allege that beginning in 2000, Crédit Lyonnais knew that its customer, CBS, was transferring money to Hamas-controlled entities. The case continues.³¹

Keren Elmaliach v. Bank of China Ltd

84 victims of Hamas rocket attacks have sued the Bank of China in the US Court for processing payments benefitting Hamas. The plaintiffs, who include family members of victims of terrorist bombings and rocket attacks carried out by Palestinian Islamic Jihad and Hamas in 2006 and 2007, are claiming that the Bank of China aided and abetted the attacks by providing wire transfer services to both terror groups. They allege that a Hamas operative received money into his account from Hamas’ headquarters in Syria and then transferred it to Gaza. The plaintiffs argue that the bank should have seen the cash transfers as a red flag and ignored a warning from the Israeli Government that the funds were being used to finance terror attacks. In 2011, Bank of China lost the argument that the US was not the best forum for the complaint. The Case continues.³²

Gill v. Arab Bank

In a civil litigation action filed in, 2011, a resident of Israel, Mati Gill, sued Arab Bank for damages under the Anti-Terrorism Act for injuries he sustained in an alleged terrorist attack that occurred in Israel in

2008. Gill alleged he sustained wounds as a result of gunfire shot from Gaza into Israel that he attributed to Hamas. In his complaint, Gill asserts the bank acted recklessly, knowingly or intentionally in processing financial transactions that benefited individuals and organisations that were allegedly affiliated with Hamas, and that this contributed to Hamas ability to conduct terrorist attacks.³³ On 12 September 2012, Senior Judge Jack B. Weinstein found the plaintiff failed to show the bank directly caused the attack, dismissing his claim that the bank aided and abetted Hamas. And then Judge Weinstein dismissed the Plaintiff’s claims in their entirety on 6 November 2012 after concluding that “the evidence does not prove that the bank acted with an improper state of mind or proximately caused plaintiff’s injury”.³⁴

Iran

Iran is the subject of multilateral sanctions, including four UN Security Council Resolutions imposing arms embargoes and asset freezes targeting persons involved in Iran’s nuclear development and terrorism support. Member states’ sanctions against Iran have in many instances exceeded the UN measures. The EU restricts payments to and from Iran and prohibits a list of commercial activities and supporting Iran’s petroleum industry and nuclear development. The US enforces a long-standing, comprehensive embargo against Iran, prohibiting US persons from providing services of any kind to Iran or its nationals and freezing assets of key Iran Government banks and parastatals.³⁵ Most recently US sanctions have imposed liability on US parent companies whose foreign subsidiaries or affiliates engage in prohibited transactions involving Iran unless the US parent and requires that the US parent divests itself from the foreign subsidiary or affiliate unless it can demonstrate that such activity was licensed.³⁵ Iran has been on the US Department of State’s State Sponsors of Terrorism List since 1984 and is the world’s most active sponsor of state terrorism, according to the US Government.³⁶ US authorities maintain that Iran is allowing Al-Qaeda to use Iran as a transit point for money, arms and fighters based in Pakistan and Afghanistan.³⁷ The Quds Force, the external operations branch of the Islamic Revolutionary Guard Corps, has provided weapons, training, and funding to Hamas, Palestine Islamic Jihad, the Taliban in Afghanistan, and Iraqi Shia militant groups that targeted US and Iraqi forces.³⁸ Following Israel’s invasion of Beirut in 1982, Iran supported the creation of Hezbollah with the arrival in Lebanon of 1,500 Islamic revolutionary guards from Iran, and remains a close ally and financial supporter. Senior IRGC, IRGC Quds Force, and Iranian Government officials were indicted by the Government of Argentina for their alleged roles in the

1994 terrorist bombing of the Argentine-Jewish Mutual Association.³⁹

US Sanctions

Relations between the US and Iran turned hostile following the 1979 revolution in which Iran's Shah was deposed and replaced by an Islamic republic. A group of Islamist militants took over the American Embassy and held 52 Americans for over a year. In response, the US restricted transactions between US persons and Iran, and blocked Iranian property. In 1981, the US and Iran reached an agreement, known as the Algiers Accords, which led to the release of the hostages and the unfreezing of most Iranian assets. Some property of the Government of Iran remains frozen.⁴¹

In the 1980s the US-Iran relations deteriorated as a result of Iran's support of terrorist groups and the US involvement in Middle East affairs including the Iran/Iraq war and Lebanon. The US imposed import/export restrictions involving Iran in 1987, following attacks on American forces and Kuwaiti vessels flying the American flag in the Persian Gulf. Additional grounds for the sanctions were Iran's continued support of Hezbollah, which abducted over 90 hostages from 21 nations in the 1980s to force an end to US involvement in Middle East conflicts. Hezbollah was responsible for suicide bombings against American targets in 1983 and 1984 on two US Embassies in Beirut and the US Marine peacekeepers barracks.

In the 1990s US attempted an aggressive expansion of its sanctions against Iran amidst fears of Iran's continued terrorism support and development of weapons of mass destruction. In 1995, US President Clinton imposed a full embargo against Iran as part of a "Dual Containment" policy aimed at both Iran and Iraq. One catalyst was intelligence reports that Iran was acquiring components for nuclear weapons. These sanctions followed EU countries' criticism of the US for continuing to import Iranian oil while they had been pressured to cooperate with the US containment policy.⁴² In 1996, the US Congress passed the Iran and Libya Sanctions Act (ILSA) to reduce Iran's ability to export oil and gas and thus deny funds for the development of WMD and support of international terrorism. ILSA required the President to impose at least two out of a menu of six sanctions on foreign companies (entities, persons) that make an investment of more than \$20 million in one year in Iran's energy sector. The law gave the President the ability to assert a waiver of sanctions to serve US national security interests.⁴³ The EU reaction to ILSA was decidedly negative, and in 1996 it adopted "blocking legislation" to prevent EU companies and their subsidiaries from

complying with ILSA.⁴⁴ In addition to encouraging member states to impose their own sanctions on companies complying with ILSA, the EU decided to lodge a complaint against the US with WTO.⁴⁵ This 1996 US statute was not enforced as the US Congress expected. French company Total signed contracts with Iran for the development of oil fields prior to the passage of ILSA in 1995 and after ILSA was in effect in 1997, the latter being for the development of part of the South Pars field with partners Gazprom and Petronas. The US Congress pressured the US President to enforce ILSA. However, the US State Department announced an ILSA waiver for Total, noting France's cooperation to combat terrorism and WMD developments in Iran, and indicated that the waiver would be used in similar situations. Another of the administration's concerns was the potential for other countries to impose reciprocal sanctions against US corporations.⁴⁶ In 1997, the US and the EU formally agreed to try to avoid a trade confrontation over ILSA.⁴⁷

Nuclear Threat and Multilateral Sanctions

The concern for Iran's support of terrorist groups grew with concerns about Iran's nuclear ambitions. Iran's secret underground uranium-enrichment facility in Natanz was discovered in 2002 via satellite. The International Atomic Energy Agency (IAEA), the UN's nuclear watchdog, began an inspection in 2003, and the existence of weapons grade plutonium was discovered. There was fear that Iran was enriching plutonium for nuclear weapons. Its raw fuel needs for energy were supposedly already met by an arrangement with Russia as part of the Bushehr reactor project begun in the 1970s under the Shah. Iran agreed with the EU to temporarily suspend uranium enrichment.⁴⁸ However, Iran's then President Mahmud Ahmadinejad announced in 2005 Iran's plan to resume enrichment. Thereafter, Iran refused to cooperate with UN nuclear facility inspectors, and it refused to comply with the UN Security Council's demand that Iran suspend nuclear enrichment and reprocessing.⁴⁹

In response, the UN imposed four sets of sanctions, in Security Council resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010). These resolutions collectively call for cargo inspections and bans on the sale of materiel and technology related to nuclear enrichment and ballistic missile development, as well as asset freezes on individuals, banks and organisations supporting Iran's military and nuclear programmes. The asset freezes targeted those persons and agencies instrumental for Iran's nuclear development and terrorist group support.⁵⁰ Those designated included the Atomic Energy Organisation of Iran, key persons and entities of the Islamic Revolutionary Guard Corps

(IRGC) and other entities supporting Iran's nuclear development.⁵¹ Additionally, the US and EU designated some of Iran's largest banks, Bank Melli, Bank Mellat, and Bank Saderat, for having facilitated Iran's proliferation activities or its support for terrorism. The US placed sanctions on Iran's Quds Force as a terrorism supporter.⁵²

In 2008, the US blacklisted the state controlled Islamic Republic of Iran Shipping Lines (IRISL) and all of its ships in 2008. Vessels boarding by US and Israeli authorities revealed a large arms cache, including thousands of rockets, grenades and mortar shells, destined for Hezbollah. IRISL took steps to hide its connections to vessels identified on the US sanctions list. The IRISL ships' Iranian flags were changed, and vessels' names were changed.⁵³ Three new Iranian front companies took over the operation of the majority of the blacklisted ships: Hafiz Darya Shipping Lines, Sapid Shipping and Soroush Sarzamin Asatir.⁵⁴ US authorities brought criminal charges against these companies for deceiving at least nine banks into processing over US\$60mio in transactions benefitting Iran.⁵⁵ In 2009, another secret enrichment plant being built by Iran underground was exposed. This plant was being built with capacity for 3000 advanced centrifuges for enrichment near Qom - not enough for commercial use but enough for the processing of weapons grade uranium. The heavily disguised facility was in breach of a 2003 agreement with the IAEA to provide early design information for any nuclear facility construction.⁵⁶

The UN Security Council's fourth set of sanctions measures against Iran in 2010 were the strongest measures to date. In addition to weapons embargo provisions, UNSCR 1929 called on Member States to prohibit financial services (including banking and insurance) if there are reasonable grounds to believe that such services could contribute to Iran's nuclear or missile programmes. However, the resolution does not have the scope of the broad US sanctions restrictions, nor does it ban trade in oil and gas, Iran's principal source of revenue. Countries imposing sanctions against Iran following UNSCR 1929 include Canada, Australia, South Korea, Japan, India and Israel.⁵⁷

The EU's measures went further than UNSCR 1929. A goal of EU Council Regulation (EU) No 961/2010, published on 27 October 2010 was to prevent financing, services and key equipment and technology from benefitting Iran's oil and gas industry, which was recognised as integral to Iran's funding of its weapons development. In addition to an arms ban and asset freeze of identified persons, the regulation restricts trade with Iran in relation to investment; the oil and

gas industry; uranium mining; the insurance and bonds sector; the financial services industry; and transport. The most controversial part of the regulation was the restriction on transfers of funds to and from Iranian individuals and entities.⁵⁸

In 2011, Switzerland imposed sanctions against Iran similar to the EU restrictions.⁵⁹ Its military goods ban was extended to dual use goods, and certain restrictions were imposed on financing and exports supporting Iran's oil and gas industry.⁶⁰

Between 2010 and 2012, in an effort to further increase pressure on Iran to return to constructive dialogue in the wake of international concerns about the connection between its energy sectors and its nuclear programme highlighted by UN Security Council Resolution 1929, the US tightened existing sanctions against Iran and issued broader sanctions targeting the country's energy sector designed to further isolate Iran from the international financial community. First, in 2010, President Barack Obama signed into Law the Comprehensive Iran Sanctions Accountability and Divestment Act (CISADA), which amended the Iran Sanctions Act of 1996, significantly expanded the energy-related activities that are subject to sanctions unless a waiver has been received, imposed new sanctions with respect to foreign financial institutions that knowingly facilitate Iranian WMD transaction or activities and transactions with designated Iranian-linked banks and other blocked persons.⁶¹

In 2012, in what has been considered even more sweeping legislation, President Obama signed the Iran Threat Reduction and Syria Human Rights Act (ITRSRA) which expanded the types of Iran-related activities subject to sanctions. At the outset the ITRSHRA expanded the extraterritorial reach of US sanctions laws by requiring foreign subsidiaries and affiliates that are majority owned or controlled by a US person to abide by US sanctions against Iran, and holding the US parent liable for any violations committed by the foreign sub or affiliate. Previously, foreign entities were not directly bound by sanctions against Iran unless US persons were involved.⁶² Additionally, ITRSHRA requires US foreign private issuers who have engaged in activity prohibited to publicly self-disclose such activity. Any such disclosures will require the US President to initiate an investigation into whether sanctions should be imposed on the party making the disclosure.⁶³ In sum, the ITRSHRA substantially broadened the scope of activities that are subject to sanctions, targeting particularly those related to providing financial services to entities linked to the government of Iran and also broadened sanctions

against Iran's energy sector.

See also Breaking News below at the end of this Book.

Myanmar

The EU, US, Canada and Australia have imposed sanctions against the Myanmar government in reaction to the Myanmar regime's repression of its people. Since 1996, the EU has held a common position⁶⁴ imposing sanctions on Sanctions restrictions include a travel ban on top political officials, an arms embargo, a freezing of the assets of Burmese officials and their business partners, a ban on financial services and investment and restrictions on exports and imports, and cessation of trade preferences, and suspension of all aid with the exception of humanitarian aid.

The US first imposed sanctions against Myanmar⁶⁵ in 1997, when the US banned new US investment in economic development of resources in Burma because of Burma's military regime's continuing repression of the democratic opposition. The US President noted that the regime had arrested and detained large numbers of students and opposition supporters, sentenced dozens to long-term imprisonment, and prevented the expression of political views by the democratic opposition.⁶⁶ Additionally, the US President noted Myanmar's role in the drug trade as the world's leading producer of opium and heroin.

In 2003, the US⁶⁶ strengthened sanctions against the Burmese regime because of its continued human rights abuses, the detention of pro-democracy leader Aung San Suu Kyi, and its refusal to honor the election results of the 1990 People's Assembly election. On 28 July 2003, the US President signed into law the Burmese Freedom and Democracy Act of 2003 and an implementing Executive Order to prohibit the importation into the US of Burmese-origin goods, the provision of US financial services to Burma and the processing of payments involving Burma. These measures, as well as subsequent Executive Orders, froze assets of persons identified as supporting the Burmese regime.

These sanctions did not deter the regime's⁶⁷ pattern of repression. In late 2007, the Government raided Buddhist monasteries and arrested monks, the country's highest moral authority, to quell peaceful civil protests led by monks following a Government decision that caused a huge rise in the price of fuel. The EU, US, Canada and Australia each issued sanctions⁶⁸ against the regime. One of the goals of the EU and US sanctions was to take aim at the regime's dependence on, and strict control of, the sale of precious stones and other items. The EU imposed trade restrictions on items such

as timber, metals, and semi-precious stones. In 2008,⁶⁹ the US augmented its 2003 sanctions with restrictions on imports of jadeite and rubies mined from Burma (and jewellery containing these stones). Canada's sanctions were considered some of the broadest,⁷⁰ including a full export/import ban, a ban on new investment and a restriction on financial services. In 2010, the EU added more stringent⁷¹ bans on business activity and investments and freezing the assets of a broader list of individuals and entities.

Certain changes are occurring in Myanmar. In 2010, Aung San Suu Kyi was released from prison. The first legislature in 22 years was formed in 2011. However, it is believed that the sanctioned military regime will continue to control the country with an iron fist.⁷²

Burma is reported as the world's second largest producer of opium, located at the corner of the Golden Triangle. In 1996 the US Embassy in Rangoon released a "Country Commercial Guide", which states "Exports of opiates alone appear to be worth about as much as all legal exports." A four-year investigation concluded that Burma's national company Myanmar Oil and Gas Enterprise (MOGE) was "the main channel for laundering the revenues of heroin produced and exported under the control of the Burmese army."⁷³

Myanmar has become one of the main gas exporters in Asia and that Burma's oil and gas sectors are the major sources of foreign currency for the regime. Corporations operating the Yadana natural gas pipeline in southern Myanmar are making annual payments to the junta.⁷⁴ The Shwe gas project is estimated to generate royalties for the Burmese regime in the amount of an estimated US 40 billion over three decades. The pipeline will send gas from Burma's west coast to China. Human Rights groups have highlighted the pervasive use of forced labour and human rights abuses by military and civilian personnel in Burma for the Yadana pipeline and other development projects.⁷⁵

US embassy cables leaked in 2010 suggest that Myanmar was attempting to build nuclear and missile sites, with the help of North Korea.⁷⁶

In 2012, US authorities lifted sanctions against two key Myanmar officials: Burmese President Thein Sein and Lower House of Parliament Speaker Thura Shwe Mann, in acknowledgement of their reform efforts. The US also lifted the ban on conducting financial transactions and investing in Burma, but continued to prohibit dealings with the Burmese military, the Office of Procurement or rebel groups.⁷⁷ The new authorisations introduced a new reporting requirement that included

companies which invested to disclose certain internal policies and procedures relating to the investor's stance on human rights, anti-corruption and bribery among other policies.⁷⁸

Although US sanctions were also lifted on a variety of products, the prohibition and restrictions remain with regards to importing jadeite and rubies mined or extracted from Burma, including any jewellery articles that contain such gems.⁷⁹ Similarly, in 2012, the EU suspended sanctions against Myanmar for one year recognising the positive changes in Burma. The restrictions had concerned trade and investment in various industries including logging and timber, precious metals and mining and other interests.⁸⁰ Human rights groups like Human Rights Watch and the US Campaign for Burma have expressed concern that the lifting of sanctions is premature arguing that reforms promised in Burma particularly with regards to serious human rights abuses have been tenuous at best. A UN report on human rights in Myanmar also warned that progress in releasing the more than 120,000 political prisoners has been erratic. Nevertheless, countries like Australia and Canada have followed the EU and US actions by lifting some sanctions against Burma in light of the substantial democratic reforms that have taken place in the country.⁸¹

North Korea

The international community has imposed sanctions against North Korea primarily to encourage North Korea to abandon nuclear development. North Korea has been under UN sanctions since its first atomic test in 2006, and those measures now include an arms embargo, a ban on luxury goods and travel bans and asset freezes against persons supporting North Korea's nuclear development.¹

The US has imposed sanctions against North Korea, to varying degrees, since 1950, attempting a carrot and stick strategy to control the regime's behaviour by imposing sanctions, lifting sanctions and providing aid.² Current US sanctions restrictions currently in place include a limited asset freeze, export and import restrictions, ban on registration or operation of vessels operating under North Korean flag or assistance to such vessels, and a ban on certain donations from the North Korean Government.³

While North Korea is also involved in the drug trade and the production and laundering of counterfeit bills, there is limited political will to impose full sanctions against North Korea, for fear of derailing fragile negotiations regarding North Korea's nuclear development. North Korea's drug trafficking activities

don't draw the same attention as its nuclear weapons programme, but there is concern that routes established for drugs and contraband are routes that can be used for smuggling other items, including weapons-grade plutonium.⁴

In 2002, the Democratic People's Republic of Korea (North Korea) acknowledged it had clandestinely developed facilities to enrich uranium, saying it was no longer bound by the terms of a 1994 accord that froze its old plutonium-based programme. The "six-party talks" were organised in response. Beginning in 2003, North Korea participated in a series of six-nation nuclear talks in Beijing, which included China, US, Japan, Russia and South Korea.⁵

However, North Korea withdrew from those talks in 2005, citing as a reason the US imposition of sanctions against *Banco Delta Asia*. In September 2005, the US Treasury designated *Banco Delta Asia*, a Macau-based bank, as a "primary money laundering concern" because of its laundering of North Korean money from counterfeiting and drug smuggling. US banks were banned from dealing with the *Banco Delta Asia* pursuant to Section 311 of the US Patriot Act. Macau banking authorities froze 50 North Korean accounts worth over US\$20mio.⁶ North Korea conducted its first nuclear test in October 2006. As a result, UNSCR 1718 was unanimously passed. The Resolution called on member states to ban exports to North Korea of nuclear, missile and chemical weapon technology and other military equipment, a ban on the export of luxury goods, as well as an asset freeze and travel ban against persons identified as supporting North Korea's weapons development. The resolution also called for the inspection of cargo ships for weapons of mass destruction.⁷ Authorities including the EU, US, Switzerland, UK, and Australia implemented sanctions measures against North Korea. North Korea agreed to return to the six-nation talks on its nuclear programme.⁸

In 2007, North Korea signed a tentative agreement during six-party talks in Beijing to shut down its nuclear programme in exchange for over US\$250mio worth of oil and aid.⁹ However, throughout 2008, North Korea announced it would not complete the dismantling of its programme if additional concessions were not made. The US Government reduced sanctions against North Korea and removed the country from the US list of State Sponsors of Terrorism in 2008.¹⁰

In 2009, North Korea exploded another nuclear device underground and launched a long-range missile over Japan and into the Pacific Ocean.¹¹ The UN Security Council issued UNSC Resolution 1874 (2009)

extending the arms embargo and calling on member states to prohibit financial services that could contribute to North Korea's nuclear or ballistic missile related programmes.¹² The EU created its own sanctions regime against North Korea, separate from UNSCR 1874, in the form of a regulation targeting close associates of Kim Jong Il. North Korea stated that the "US-led" sanctions were an act of war and that it planned to deploy its plutonium supply for military use.¹³

In 2010, the US banned the export of luxury goods to North Korea's elite, in response the 2009 nuclear test and North Korea's 2010 attack on the South Korean warship, Cheonan. 46 seamen died when the South Korean Navy ship sank off the country's west coast.¹⁴ An investigation carried out by a team of international experts from South Korea, US, UK, Canada, Australia, and Sweden concluded that the warship had been sunk by a North Korean torpedo.¹⁵ A 2010 UN report states that North Korea has been secretly supplying banned nuclear and ballistic missile components to Iran, Syria and Myanmar.¹⁶

Sudan

The US has enforced a comprehensive embargo against Sudan since 1997 for the Sudanese Government's support for international terrorism, ongoing efforts to destabilize the region, and human rights violations. The US sanctions prohibit virtually all transactions with the Sudanese government or where ultimate benefit is into Sudan, and imposes extensive controls on the exportation of US origin goods and technology to Sudan.¹⁷ Sudan has been on the US list of state sponsors of terrorism since 1993. It has housed terrorist bases and terror training camps since the 1990s when bin Laden and followers based operated training and financial operations from Khartoum. Following US Embassy bombings in Kenya and Tanzania in 1988, the US destroyed a facility in Sudan associated with chemical weapons and the bin Ladin network. While the Sudanese government has more recently cooperated with anti-terrorism efforts, it remains on the US list of Sponsors of Terrorism, primarily because of its inability to prevent groups such as Al-Qaeda and Hamas from using Sudan as a logistics base for operations. The Lord's Resistance Army conducted attacks in border areas in 2010, displacing 25,000 southern Sudanese. There is also evidence that Sudanese extremists have participated in terrorist activities in Somalia.¹⁸

The 2003 Darfur conflict compelled the UN Security Council to impose sanctions measures against Sudan that included an arms embargo and asset freeze against certain Sudanese officials responsible for the violence. Rebel groups in Darfur took up arms, accusing the

Sudanese government of oppressing non-Arab Sudanese in favor of Sudanese Arabs. The Sudanese government used oil revenues to employ advanced weaponry for use against civilian villages, and employed the Janjaweed to combat the rebels. The conflict caused mass migration, starvation, and rampant human rights abuses.¹⁹ In 2004-2006, the UN Security Council issued resolutions condemning human rights violations in Sudan's Darfur region and, in particular, the continuation of violence against civilians and sexual violence against women and girls.²⁰ The UK, Switzerland, Australia, Canada, New Zealand, Singapore and the US imposed targeted sanctions to implement the measures.²¹ The Darfur Conflict has connections to the tensions that gave rise to the Second Sudanese Civil War. In the late 1970s and early 1980s, oil had been discovered at the north-south border. Islamic fundamentalists in the north were not happy with the autonomy given to the non-Islamic majority in Southern Sudan under a prior agreement. In 1983, President Nimeiry declared all Sudan an Islamic state, terminating the Southern Sudan Autonomous Region. The civil war raged on for 22 years and resulted in over 2 million deaths.

A Comprehensive Peace Agreement (CPA) between north and south was signed on 9 January 2005 in Nairobi. Elements of the agreement include merger of military forces and a sharing of oil revenues and jobs, and the option of an autonomous South to opt out of Sharia law imposed in the North.²² On 9 July 2011, Southern Sudan became an independent state, as a result of a January 2011 referendum that took place as part of the CPA.²³ The new state formed by Southern Sudan is largely exempt from the US sanctions against the Government of Sudan. However, US persons (wherever located) are still prohibited from dealing in property and interests in property of the Government of Sudan, performing services that benefit Sudan, engaging in transactions relating to the petroleum or petrochemical industry in Sudan, and participating in exports to or imports from the new state that transit through Sudan. For example, US persons would not be able to facilitate payments from the new state to the Government of Sudan from the sale of Southern Sudanese petroleum as a result of a revenue-sharing arrangement.²⁴ Sudanese armed forces continue to threaten the peace with attacks on civilians in rebel-held areas, actions which human rights groups are calling war crimes.²⁵

Syria

Several governments have sanctioned Syrian government officials and agencies responsible for crackdowns on Arab Spring insurgents in 2011. In January of 2011, protesters began calling for political reforms and the

reinstatement of civil rights, as well as an end to the state of emergency which has been in place since 1963, to which the government responded with a series of bloody crackdowns. Many tens of thousands have died in the conflict²⁶ already. In 2011 the EU, Switzerland, Australia, Canada, and the US imposed an arms embargo, asset freezes and/or travel bans against Syrian President Bashar al-Assad and other senior Syrian officials, and Syrian government agencies. Additionally, the EU and US specifically sanctioned the Iranian intelligence services and commanders for providing equipment and support to help the Syria regime suppress protests.²⁷ As government violence against insurgents increased in 2011, the EU amended its sanctions measures against Syria to include a ban on importing or purchasing from Syria crude oil or petroleum products, as well as related transactions concerning transport, finance and insurance to include Syrian government property; a ban new investment in Syria; prohibiting services of any kind to Syria; and banned the dealing in petroleum or petroleum products of Syrian origin.²⁸

The ban on services prohibits financial services, including processing of payments, involving individuals and entities domiciled in Syria. These sanctions are akin to the US sanctions embargo against Iran and arguably prohibit, for example, accounts for individuals. Also, they prohibit the processing of trade transactions involving Syrian vessels or transhipments through Syria. The service ban makes the US sanctions against Syria broader in scope than sanctions imposed by the US against other regimes opposing Arab Spring protests.²⁹ For example, US 2011 sanctions against the Libyan government did not prohibit services involving all Libyan nationals. This US embargo is imposed on top of those US sanctions imposed against Syria for its terrorism support.³⁰ Designated by the US in 1979 as a State Sponsor of Terrorism, Syria has provided safe-haven as well as political and other support to a number of designated Palestinian terrorist groups, including Hamas, Palestinian Islamic Jihad (PIJ), the Popular Front for the Liberation of Palestine-General Command (PFLP-GC), as well as to Hezbollah in Lebanon. The operational leadership of many of these groups is headquartered or sheltered in Damascus. Syria allows terrorist groups resident in its territory to receive and ship goods, including weapons, in and out of the country. Weapons flow from Iran through Syria, and directly from Syria, to Hezbollah.³¹

In 2004, the US imposed tailored sanctions against Syria in response to actions by the Government of Syria in support of international terrorism, its occupation of Lebanon, its pursuit of weapons of mass destruction

and missile programme, and its actions to undermine US efforts to stabilize Iraq. Those sanctions included a ban on exports and re-exports to Syria, Syrian air flights and an asset freeze against persons supporting the Syrian governments terrorism support or weapons development.³²

In 2005, a terrorist bombing in Beirut, Lebanon killed 23 people, including former Lebanese Prime Minister Rafiq Hariri. Noting the involvement of high ranking Syrian government officials in the assassination plan, the UN Security Council adopted Resolution 1636, to freeze funds and economic resources of persons identified by the Security Council as suspected of involvement in the bombing. No targets were designated under these UN sanctions.³³ In 2005 and 2006, the EU and the US issued similar measures in response to the bombing.

In 2008, the US targeted persons benefitting from corruption under the Assad regime, in particular the cousin of Assad, Rami Makhluf, who used his close ties to the Assad regime to obtain improper business advantages in a number of industries. The justification for the sanctions was that corruption and cronyism entrenched a regime pursuing oppressive and destabilizing policies, including beyond Syria's borders, in Iraq, Lebanon, and the Palestinian territories.³⁴ Terrorism concerns have escalated in 2011 with the IAEA's announcement that Syria is building secret nuclear facilities capable of refining plutonium, which can be used to arm nuclear warheads. Syria has refused to cooperate with IAEA inspections. Syrian president Al-Asad has been a staunch defender of Iran's policies, including Iran's nuclear ambitions.³⁵ Syria's financial sector remains vulnerable to terrorist financing. An estimated 70% of all business transactions are conducted in cash and as many as 80% of all Syrians do not use formal banking services. Despite Syrian legislation requiring money-changers to be licensed by the end of 2007, many continued to operate illegally in Syria's vast black market, which is believed to be as large as Syria's formal economy. Regional hawala networks remained intertwined with smuggling and trade-based money laundering facilitated by corrupt customs and immigration officials raising significant concerns that the Syrian government and business elites could be complicit in terrorist financing schemes.³⁶

Finally, in 2012, the US under ITRSHRA, expanded sanctions against Syria focusing on human rights abuses reported to have been committed by the Assad regime against the Syrian people as a result of the two and half year conflict with rebel forces determined to force Assad to relinquish power.³⁷

Venezuela

With the death of President Chavez it remains to be seen how his successor, Nicolas Maduro, will be seen or act, whether Venezuela continues as before or charts a new less confrontational course. As a result of former President Chavez's actions the US has sanctioned certain high level Venezuelan officials for support of narcotics trafficking and terrorism groups, and has criticised Venezuela for supporting narcotics trafficking and terrorist groups and fostering an alliance with Iran. Venezuela is recognised as one of the principal drug-transit countries in the Western Hemisphere, located between the world's largest cocaine producer, Colombia, and the world's largest consumer of cocaine, the US.³⁸ A US Government Accountability Office (GAO) study reported a high level of corruption within the Venezuelan Government, military and law enforcement that has allowed that country to become a major transshipment route for trafficking cocaine out of Colombia.³⁹

In September 2011, US Government sanctioned four Venezuelan political figures, including military officers and Government officials political figures associated with Venezuelan President Hugo Chavez, for providing training and weapons and to the leftist Revolutionary Armed Forces of Colombia (FARC) and supporting the rebel group's narcotics and arms trafficking activities.⁴⁰ The FARC is a Colombian terrorist insurgency group that finances its operations through narcotics trafficking, extortion and kidnapping, and the US Government has designated it as a terrorist organisation.⁴¹ One of the four sanctioned individuals was a primary arms dealer for the FARC and a main conduit for FARC leaders based in Venezuela, according to the US Government. Two of the four used military and intelligence positions to establish an arms-for-drugs route with the FARC and coordinate security for the guerrillas.⁴² In 2008, the US government designated three high ranking Venezuelan officials as drug kingpins for providing material support to the FARC. The individuals were accused of protecting drug shipments and providing weapons and funding to the FARC. Venezuelan President defended the officials, and remained in office after the designations.⁴³ Hezbollah maintains a presence in Venezuela for fundraising activities. In 2008, the US designated Venezuelan diplomat Ghazi Nasr al Din for using his position to provide financial support to Hezbollah.⁴⁴ Also in 2008, Colombian authorities took action against a drug and money laundering ring in an international operation that included the capture of three people suspected of shipping funds to Hezbollah.⁴⁵ Venezuela and Iran are deepening a strategic alliance. Iran opened a bank in Caracas under the name Banco Internacional de Desarrollo C.A., an independent subsidiary of Export

Development Bank of Iran. In 2008, US Treasury's Office of Foreign Assets Control imposed economic sanctions against both banks for providing financial services to Iran's Ministry of Defence and its Armed Forces Logistics—the two Iranian military entities tasked with advancing Iran's nuclear ambitions.⁴⁶

President Chavez had opposed multilateral sanctions against Iran and has signed cooperation agreements with Iran in areas including, oil and gas, trade, and construction.⁴⁷ Media sources indicated that Iran maybe placing medium range missiles in Venezuela and Venezuela has agreed to allow Iran to establish a military base manned by Iranian missile officers,⁴⁸ soldiers of the Iranian Revolutionary Guard and Venezuelan missile officers. Venezuelan Government confirmed in 2009 that Iran was assisting Venezuela in the detection and testing of Venezuela's unmined uranium deposits.⁴⁹

Zimbabwe

Robert Mugabe has been in power since Zimbabwe's independence in 1980. Targeted sanctions have been imposed by the international community against Robert Mugabe and his associates.⁵⁰ In 2001, the US implemented under the US Democracy and Economic Recovery Act, which bars Zimbabwe from access to credit and debt reduction/indebtendness.⁵¹ Asset freezes and travel bans have been imposed by EU, US, Canada, Switzerland, and Australia. Since 2002, nearly 200 people who make up Mr. Mugabe's inner circle have been sanctioned, along with farms, agencies and corporations controlled by them.⁵²

Zimbabwe is also subject to an arms embargo. The US, EU and Canada restrict transfers of defence items and services to Zimbabwe.⁵³ NGOs have reported over the last decade grave human rights violations occurring under including arbitrary arrests, torture, censure of the press, and violent disruption of peaceful protests. Massive intimidation techniques have prevented free and fair elections. In 2005, NGOs accused Mugabe of rigging of the March parliamentary elections. The country's drought weary populace is made to fear that a vote for the opposition would result in violence or withholding of food aid. In 2008, Mugabe won the elections to his sixth term after his opponent, Morgan Tsvangirai, dropped out of a runoff election because Government enforcers were beating and killing his supporters. Various governments strengthened sanctions in response to this event, despite the fact that a power sharing agreement between the opponents was subsequently reached.⁵⁴

Russia and Ukraine

See also Breaking News below at the end of this Book.



Section 4 Money Laundering Prevention Programmes

- Risk Based Approach, 283
- Risk Assessment, 285
- AML Programme, 295
- Sanctions Programme, 301
- Anti-Bribery & Corruption Programme, 306
- Anti-Fraud Programme, 310

Risk Based Approach

Whilst AML programmes should always reflect applicable legal and regulatory requirements, programme design should also seek to strike a balance between protecting the organisation's reputation, preventing and detecting money laundering with the need to ensure that legitimate business can continue to operate and expand and that honest law-abiding customers are not treated as suspected criminals. This balance is difficult to achieve but can only be done by careful analysis of the risks and vulnerabilities, for example, represented by particular customers, products and services and channels or jurisdictions or alternatively appropriate risk scenarios to a particular financial institution. Risk will always be present and it is impossible to create a situation where incidents will not occur and to attempt to do so would unduly constrain business and commerce. An effective and proportionate AML Framework therefore needs to target resources at those areas that are considered to represent the highest risk to an institution, with less, though adequate resources and scrutiny proportionately covering areas of lesser risk.

With an "all crimes" model recently adopted by FATF in 2012, AML frameworks should also consider the threats posed by the other predicate offences, for example see Part 1, Section 1, Predicate Crimes above, but also take note of any National Risk Assessments and prioritised areas of concern, and internal Risk Assessments, which for more details see below in this Section.

In addition to AML Frameworks or tailored AML Programmes, bespoke programmes should also focus on Sanctions Compliance, Anti-Bribery and Corruption and Anti-Fraud Programmes. Market Abuse Programmes usually form part of separate Compliance Programme but require attention and emerging is a need to consider a bespoke tax compliance programme. Terrorism Finance and WMD Proliferation Programmes are usually included with AML and Sanctions Compliance Programmes. For more details on these again see later in this Section.

Increasingly, many policymakers, regulators and AML professionals recognise that an approach (known as the risk based approach or RBA) is an effective and appropriate method of mitigating risk. Indeed FATF have enshrined the RBA in Article 1¹ of their revised 40 Recommendations in 2012 demonstrating the importance for countries and the public and private sectors. Whilst some jurisdictions have failed to adopt a RBA and retain a largely rules based approach to AML, they are increasingly in the minority. In some areas, such as Sanctions

Compliance or Terrorism Finance for example, there is more a reluctance to adopt an RBA and frameworks are largely based on prescriptive rules, creating a situation where institutions have a firm set of obligations and where a "zero failure" approach is the aspiration. Even here many institutions will supplement compliance with prescribed rules with further measures utilising elements of an RBA where risks can be identified and should be mitigated. Ironically, a rules based approach can be easier for the AML professional to work within given that it sets prescriptive standards that every institution must follow and it is therefore, clear to an institution what needs to be done and about what resources are needed to meet the obligations. A fully adopted RBA offers flexibility but can create a situation where threats, risks and counter measures are assessed differently from one institution to another. It is important that institutions retain this flexibility and should not be second guessed provided such a framework is reasonable and proportionate and takes into account the particular circumstances of that institution. Policy makers and regulators have here a challenge as there are not clearly stated rules against which they can judge an institution's performance, rather they place focus on the arrangements in place to prevent financial crime (which usually includes AML, Sanctions, Anti-Bribery & Corruption (ABC) and Fraud).

Under a rules based approach it is fairly clear whether or not an institution has met its obligations but the risk based framework means that assessing the level of compliance is less clear. For institutions, this can present a significant danger in that regulators who visit a number of different institutions may select what they regard as examples of "best practice" and then expect to see this replicated in other institutions irrespective of the other internal factors that should and must be considered before such a considered assessment can be made.

Often these "best practice" assessments and statements are simply assessments of "common practice" in other words, simply because a number of institutions are doing something in a particular manner it is assumed that this represents "best practice". Whilst "common practice" can be a guide to adopting new methods, the danger is that conventional wisdom is the architect of future AML framework design. Much common practice is designed to protect an institution against regulatory criticism and not always directed towards money laundering prevention. In reality, each institution must take the evidence it has available and make its own decisions based on the information it has, the customers it serves and the product and delivery channels which it supports. Given that peer assessment becomes a real guide for regulators, it becomes imperative that institutions

document their decisions, record the evidence that was reviewed, periodically revisit those assumptions and, wherever possible and practical, benchmark their assessments with other institutions.

Determining risk is neither a static discipline nor is it one that remains constant as it will continue to be influenced by external developments including political priorities or regulatory changes, business changes and changing criminal behaviour. For that reason, it is imperative that a framework is created within which such assessments and decisions can be made such that the framework can respond. The mechanism for assessing changes in risk and corresponding responses is the Risk Assessment.

Increasingly financial institutions will undertake Risk Assessments employing detailed models using both numerical assessments of relative, comparative or changing risks across a number of risk categories, for example, customer, country, products and services and channels and/or by using scenario based assessments and control effectiveness approaches.

Once risks are identified, how to combat them will be the responsibility of the financial institution. Of course, where legal and regulatory requirements exist, these will be followed but over and above this, a financial institution will adopt a risk based approach and so make a judgement as to the focus of its control environment and as to how many resources their programmes require to run effectively and efficiently. In justifying focus and spend, a financial institution should expect to be able to explain this but not to have this second guessed. The risk of legal or regulatory censure is usually a significant driver in making risk based choices but financial and reputational damage are also important. All are inextricably linked. Taking a Risk Based Approach therefore involves complying in full with applicable laws and regulations and acting beyond that on the basis of a firm's own definition of risk appetite and priorities, whilst remaining as competitive in the market place as possible.

The following programmes highlight the areas of coverage for AML Sanctions, Anti-Bribery and Corruption (ABC) and Anti-Fraud Programmes. Before each though comes, as it should, the Risk Assessment.

Risk Assessment

There is no shortage of literature on the (in)ability of human beings to assess risk properly. Collectively we have short-term memories along with a disinclination to forego short-term gains when we perceive risks to be distant or unlikely. The literature of how people view risk depending on context, group size and numerous other factors is extensive. Quantitative models have proven to be extremely useful in helping us quantify risks, understand observed phenomena, explore the sources and impacts of financial risks and develop tools and methods for managing risks. At best, models remove a great deal of bias and subjectivity from risk analysis as well as give us a measurement tool. The Basel Committee on Banking Supervision issued in June, 2013 a Consultative Document, entitled "Sound management of risks related to money laundering and financing of terrorism"¹ which includes the following on the importance and conduct of Risk Assessments.

"Sound risk management requires the identification and analysis of ML/FT risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML/FT risks, a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied. The policies and procedures for CDD, customer acceptance, customer identification and monitoring of the business relationship and operations (product and service offered) will then have to take into account the risk assessment and the resulting risk profile of the bank. A bank should have appropriate mechanisms to document and provide risk assessment information to competent authorities such as supervisors. A bank should develop a thorough understanding of the inherent ML/FT risks present in its customer base, products and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business. This understanding should be based on specific operational and transaction data and other internal information collected by the bank as well as external sources of information such as national risk assessments and country reports from international organisations. Policies and procedures for customer acceptance, due diligence and on-going monitoring should be designed and implemented to adequately control those identified inherent risks. Any resulting residual risk should be managed in line with the bank's risk profile established through its risk assessment. This assessment and understanding should be able to be demonstrated as required by, and should be acceptable to, the bank's supervisor".

Risk Assessments have long been an expectation for example in the US where guidance can be found in the Federal Financial Institutions Examination Council ("FFIEC") BSA / AML Examination Manual,² where it is stated that management should:

...structure the bank's BSA/AML compliance program to adequately address its risk profile, as identified by the risk assessment...develop the appropriate policies, procedures, and processes to monitor and control BSA/AML risks. For example, the bank's monitoring systems to identify, research and report suspicious activity should be risk-based, with particular emphasis on higher-risk products, services, customers, entities, and geographic locations as identified by the bank's...risk assessment."

In Canada, FINTRAC, the Canadian FIU sees an AML Risk Assessment as one of the fundamental components of the risk based approach and a critical pillar in designing and implementing an AML Compliance Programme.³

In Australia, Austrac, cites four phases of an AML Risk Assessment: (i) Risk Identification; (ii) Risk Assessment; (iii) Risk Treatment; and (iv) Monitoring and Review and also provide tables and examples of how risk assessments can work.⁴

In the UK, The Joint Money Laundering Steering Group Guidance Notes outlines some of the considerations that should be taken into account when conducting a risk assessment, with taking a risk based approach being a core theme.⁵

1. The purpose of a Risk Assessment

The key purpose of AML risk assessment is to identify potential and specific money laundering risks facing a FI and how these risks are mitigated, by employing a structured methodology using both qualitative and quantitative analysis. The results of a risk assessment can be used for a variety of reasons, including:

- identify gaps or opportunities for improvement in AML policies, procedures and processes;
- make informed decisions about risk appetite and implementation of control efforts, allocations of resources, technology spend, etc.;
- assist management in understanding how the structure of a business unit or business line's AML compliance programme aligns with its risk profile;
- develop risk mitigation strategies including applicable internal controls and therefore lower a business unit or business line's residual or net risk exposure;
- ensure senior management awareness and reporting;

- ensure regulatory awareness and reporting; and
- assist management in ensuring that resources and priorities are aligned with its risks.

2. Frequency of Assessment and Periodic Updates

Undertaking an Enterprise-wide risk assessment is a complex and resource-intensive task. However, in order to fully appreciate the risk environment it is necessary to undertake one of these. The periodicity of the enterprise-wide risk assessment will depend upon a number of factors including: the type and extent of interim validation / verification that is undertaken; the results of the risk assessment; internal or external risk events; etc. Smaller FIs or FIs with an immature AML framework may choose to complete an enterprise-wide risk assessment annually, whilst this is likely to be too resource intensive for larger FIs.

Regardless of the frequency of an enterprise-wide risk assessment is undertaken, FIs are usually required to report annually on the status of the AML risk environment. This can take the form of the Annual Report or other reports. As such, one approach is to undertake a trigger-based interim validation, looking to highlight whether there has been any change to the risk environment that was previously identified. Any changes may result in the initiation of additional workstreams or highlight a need to undertake a more in-depth assessment. Additionally, ad hoc risk assessment may be performed, focusing on higher risk areas and the specific controls that have been implemented to address the given risk. The results from these ad hoc risk assessments can then be incorporated into the next regular AML risk assessment.

Whichever approach is chosen, FIs should ensure that their approach is clearly documented and approved by senior management. The methodology for the risk assessment must be clearly articulated, especially with regard to the bases for its conclusions, e.g. scoring / weighting, etc.

3. Ownership, Roles & Responsibilities

Senior management at a FI are overall owners of the risk environment and usually delegate the assessment of AML risk to the Legal and/or Compliance / AML Unit, who will usually have primary responsibility for the initiation and delivery aspects of the AML Risk Assessment, including methodology development, maintenance, periodic process / activity initiation and record keeping of completed assessments. Business line heads as well as other departments, e.g. IT, will also be required to contribute. The purpose of the risk assessment and the contribution required should be clearly outlined, with FIs considering whether to include spe-

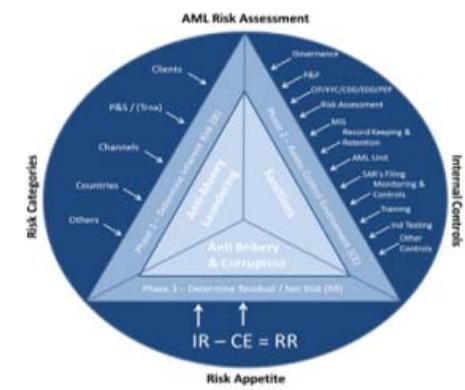
cific responsibility for the execution of and contribution to the risk assessment as part of the annual objective setting process for relevant staff

4. AML/Sanctions/Anti-Bribery & Corruption (ABC)

AML compliance units at most FIs will manage AML, Sanctions and ABC within a single department. As such, firms may choose to cover all three areas within a single risk assessment or more usually by three separate assessments, or a combination, for example, a combined AML and Sanctions Risk Assessment and a separate Anti-Bribery Risk Assessment. The same can be said for Fraud, though some FIs treat Fraud often as a distinctly separate risk management taxonomy whilst others see benefits in closely aligning the approaches. Areas such as insider dealing and market manipulation, increasingly becoming predicate offences to money laundering is usually assessed as part of the non-financial crime risk assessments conducted within an FI, usually by Compliance, separate from AML Compliance though approaches will be similar.

5. Conventional/Standard AML Risk Assessment Model

Whilst there are numerous ways to conduct Risk Assessments, increasingly the most common used by FIs can be described as the "conventional/standard model." The following diagram illustrates the practice:



In this Model a firm will apply an adopted methodology performing a structured approach to conducting a risk assessment. The risk assessment should cover the entirety of the business of the firm though may be conducted in parts or as part of a rolling cycle to focus on separate areas, e.g. divisions, units or specific business lines. The risk assessment should consider all

relevant inherent money laundering risk factors in order to determine its risk profile and in turn assess the nature of mitigating controls both from a design and operating effectiveness standpoint in order to arrive at the residual or net risk, which should be within the firm's established risk profile, essentially the firm's risk appetite. Whilst the Risk Assessment is the responsibility of the firm, the money laundering risk assessment will be designed and carried out usually by the competent AML unit, applying specialist knowledge and expertise alongside gathering relevant external and internal information. The risk assessment process can be considered in three Phases: Phase 1: Determine the inherent risk; Phase 2: Assess the internal control environment (both design and operating effectiveness); and Phase 3 Determine the residual/net risk.

Phase 1 – Inherent Risk Assessment

As no two firms are the same, inherent risk ratings may vary for financial institutions depending upon the size and scope of their businesses and the risks involved. In order to identify the particular inherent risks for a particular financial institution inherent risk across five risk categories are commonly employed which are described as follows:

1. **Clients;**
2. **Products and Services;**
3. **Channels;**
4. **Geographies; and**
5. **Other Qualitative Risk Factors.**

Risk categories are broad types of areas of risk faced by an organisation. These broad risk categories are then sub-divided into inherent risk factors that are derived from regulatory guidance or interest and industry leading practices. These multiple risk factors are included in each risk category and include a mix of both qualitative and quantitative criteria. Risk factors are the underlying causes or circumstances that led to reputation risk, regulatory or legal sanction and possible subsequent financial costs. Due to the nature of the particular business unit or business line's products and services and customer base, a risk based approach is used to calculate inherent risk. Each risk factor is assigned a score/ weighting which reflects the level of risk associated with that risk factor and the prevalence of that risk compared to the other risk factors.

Client Risk

For the purposes of assessing the inherent money laundering risk of a business division, unit or business line, the customer base and business relationship should be assessed. A number of client forms, industries, activities, professions and businesses, alongside other factors,

for example, perhaps the length of a client relationships can increase money laundering risks. The following categories can be used to stratify the customer base and to identify relative risks, which focus on client type, ownership, industry, activity, profession and/or business. Some or all of these categories may be relevant depending upon the particular division, unit or business line under review. Different customer types are assigned different risk scores depending upon the relative risk they pose. Each client type is assigned a risk score, depending upon the expected amount of AML risk, it carries relative to each other. For the business division, unit or business line in question, the volume (#) of clients that fall within each client type should then be determined/estimated. This data can be utilised to determine what percentage (%) of each business division, unit or business line client types are rated low risk versus moderate, versus high, versus higher risk, in order to determine the overall inherent client risk. A table of inherent risk scores for different client types is set out below:

Client Inherent Risk Ratings - Example 1

Clients (1) - Persons	Ratings
Individuals	
- High Net Worth	High
- Retail	Low
- Other	Mod
Entities	
Publicly Held Companies	
- Recognised Stock Exchange	Low
- Not Recognised Stock Exchange	High
Privately Held Companies	
- Operating Company	Low
- Non-Operating Company	Mod
- Bearer Share Company	High
Government Entities	
- Domestic/Low Risk Country	Low
- Moderate Risk Country	Mod
- High Risk Country	High
- Higher Risk Country	Higher
Financial Institutions/Banks and Reg Brokers	
- Recognised Stock Exchange & Compliant Country	Low/Mod
- Not-Recognised Stock Exchange and/or not Compliant Country	High/Higher

Client Inherent Risk Ratings - Example 2

Clients (2) - Special Categories with Increased Risks	Ratings
Politically Exposed Persons	
- Domestic	High
- International	Higher
Industry / Activity	
- Cash-Intensive Businesses	Med
- Money Services Business	High
- Charities & Non-Profit Organisation	High
- Intermediaries/Commission Agents	High
- Real Estate Agents	High
- High Value Goods Dealers	High
- Precious Metals & Stone Dealers	High
- Gatekeepers	High
- Casinos incl Internet Gambling	High
- Arms Dealers	High
- Private Military Firms	High

See Part 1, Section 2, Sub-section 2, Customer Risks

Products and Services Risk

Alongside "Clients" one of the other major risks is Products and Services Risks, where a financial institution will seek to identify its full portfolio of main products/account types and assign an inherent score, for example, low, moderate, high or higher to each main product/account type, based on its general inherent characteristics, and the degree of money laundering risk present relative to the other business products/account types.

For the business division, unit or business line in question, the volume (#) of products/ account types offered by the business, and (if available), associated account balances or where relevant turnover should then be determined/estimated.

This data can be utilised to determine what percentage (%) of each business division, unit or business line products/ account types are rated low risk versus high risk, in order to determine the overall inherent product risk.

A table of inherent increased risk scores for different Transactions and Product/Services is set out as follows:

Transactions Inherent Risk Ratings - Example

Increased P&S Risks (Transactions) 2	Rating
Significant/Unusual Cash/Cash Like	High
Pass-throughs	High
Unusual Wire Transfers	High
Smurfing	High
Suddenly Active	High
Other Unusual/Suspicious	High

Products & Services Inherent Risk Ratings - Example

Increased Products & Services Risks 1	Rating
Alternative Investment/Structured Products	Mod/ High
Trade/Export Finance	Mod/ High
International Private Banking/WM	High
International Correspondent Banking	High
- International Wires	High
- Pouch Services	High
- Precious Metals (Physical Delivery)	High
- Banknotes/Bulk Cash	High
- Payable-through Accounts	High
- Downstream Clearing	High
- Special Use Accounts	High
- International Brokered Deposits	High
Safe Deposit Services	High
Precious Metals (Delivery) Services	High
Unlimited Cards	High
Benchmark Indices Setting	High

See Part 1, Sections 2, Sub-section 3, Products & Service (incl Channels) Risks

Channels Risk

Some delivery channels/servicing methods can increase money laundering risk because they increase the risk that the division, unit or business line as appropriate does not truly know or understand fully the identity and activities of the Client. Consequently it should be assessed whether and to what extent the method of account origination or account servicing, such as anonymous account opening or the involvement of third parties, including intermediaries could increase the inherent money laundering risk.

For this risk category the business division, unit or busi-

ness line will then determine / estimate the percentage (%) of accounts that are rated low risk versus moderate, versus high versus higher risk, in order to determine the overall inherent channels risk.

An example table of inherent risk scores for different Channels risk factors is set out as follows:

Inherent Risks for Channels Risks - Example

Channels Risk	Rating
Account Origination	
Solicited	Low
Unsolicited (incl walk-ins, mail-ins etc)	High
Account Servicing	
Face-to-face	Low
Only non-face-to-face (incl mail, phone, text, video, internet)	High
Only non-face-to-face via Intermediary incl Gatekeepers	Mod
See Part 1, Section 2, Sub-sections 1, 2 & 3	

Geography/Country Risk

Identifying geographic locations that may pose a higher risk is a core component of any inherent risk assessment and the business division, unit or business line will seek to understand and evaluate the specific risks associated with doing business in and/or opening and servicing accounts and/or offering products and services and/or facilitating transactions involving certain geographic locations. Geography/Country risk may also be considered together directly with some of the other risk factors in other risk categories, for example, in Clients for financial institutions, and in Products and Services for Transactions. With respect to the location of the business division, unit or business line, the geographic/ country risk will also be analyzed, which will also include its subsidiaries, affiliates and offices, both internationally and domestically. The aim is to identify what percentage are located in low versus moderate, high or higher risk geographies/countries. For clients, the aim is to identify the number (#) of its clients within each country. This data will then be utilised to determine what percentage (%) of the clients are located in low versus moderate, high or higher risk geographies/countries. In order to map geographies/countries into different risk ratings, a firm's own country risk model or equivalent third party vendor product appropriately reviewed should be utilised. It may also be useful to consider in country hotspots or regional hotspots. An example table of inherent risk scores for different Geography/Country risk factors is set out below:

Inherent Risks for Geography Risks - Example

Geographies/Country Risk	Rating
Own Bank/FI Locations	
Higher Risk Countries	Higher
High Risk Countries	High
Moderate Risk Countries	Mod
Low Risk Countries	Low
Client Locations	
Higher Risk Countries	Higher
High Risk Countries	High
Moderate Risk Countries	Mod
Low Risk Countries	Low

Other Qualitative Risk Factors

Additional risk factors can increase operational risks and contribute to an increasing or decreasing likelihood of breakdowns in key AML controls. Qualitative risk factors directly or indirectly affect inherent risk factors. For example, significant strategy and operational changes, such as the introduction of a major new product, or service, a merger or an acquisition, opening or closing in a new location, may affect the inherent risk. Whilst these changes may well require the establishment of and/or the applicability of existing or new internal controls, given that these controls may take some time to become effective, the division, unit or business line will need to assess whether the inherent risk may have temporarily increased or changed. The main "Other Qualitative Risk Factors" include:

Inherent Risks for other Qualitative Risks - Example

Other Qualitative Risk Factors	Rating
Customer Base Stability	L/M/H
Integration of IT systems	L/M/H
Expected Account/Customer Growth	L/M/H
Expected Revenue Growth	L/M/H
Recent AML Compliance Employee Turnover	L/M/H
Reliance on Third Party Providers	L/M/H
Recent/Planned Intro of New P&S	L/M/H
Recent/planned acquisitions	L/M/H
Recent Special Projects & Initiatives (eg Remediations; Eliminations of Backlogs, Offshoring etc)	L/M/H
Internal Audit or Other material findings	L/M/H

Standardised Industry Inherent Risk Ratings

Whilst business divisions, units and/or business lines' inherent risks can be ascertained by the application and aggregation of risks relating to Client, Products and Services, Channels, Geography/Country and other Qualitative Risk Factors, in many cases, unless unusual or specific additional risks are presented, it is likely that certain types of banking businesses will be rated lower than others, and alternatively, others higher of course.

Whilst standardised or relative ratings for banking businesses are useful, they should not solely be used in the absence of inherent risk assessments. For a table of standardised inherent risk ratings for the most important banking businesses, see below:

Standard Inherent Risk Ratings (Major Bank/FI Businesses) - Example

Standard Inherent Risk	Rating
Asset Management	Low/Mod
Brokerage	Mod/High
Commercial Banking	Mod-High
Correspondent Banking	High
Credit & Other Card Banking	Low/Mod
Investment Banking	Mod
Retail Banking	Mod/High
Wealth Management / PB	Mod/High

See Part 1, Section 2, Sub-section 3, Products & Services (incl Channels) Risks above

AML Control Effectiveness Categories	
1	AML Corporate Governance: Management Oversight and Accountability
2	Policies and Procedures
3	Customer Identification Programme ("CIP"); Know Your Customer ("KYC") Customer Due Diligence ("CDD") Enhanced Due Diligence ("EDD") Politically Exposed Persons ("PEP") etc
4	Risk Assessment
5	MIS / Reporting
6	Record Keeping and Retention
7	Designated AML Compliance Officer/Unit
8	Detection and SAR filing
9	Monitoring and Controls
10	Training
11	Independent Testing and Oversight; and
12	Other Controls

Within each of these areas, an assessment is made through answering a list of questions. Each question covers both aspects; i.e. (i) design and (ii) operating effectiveness and focusses on both written policies and procedures but also processes and controls and how they are carried out.

Similarly, as with inherent risk and with risk factors above, each response to questions posed and to each area is assigned a score which when aggregated reflects the relative strength of that control. Each area is then assigned a weighting based on the importance that the institution places on the area scored. Using a standard 3 tier model rating scale, the internal controls can be assessed and scored for example as either Strong; Moderate or Weak.

Legal/Compliance/AML Unit Override

After completing the assessment of the risk and control categories, legal/compliance/AML unit should conduct a data quality review and at this stage should consider whether to override the inherent risk rating or the control effectiveness rating of any factor or category. Whilst it is easier to justify an increase in the inherent risk rating and/or a decrease in the control effectiveness rating the reverse should also be possible though in either case the model may need to be reviewed if the changes are very significant. In all cases the rationale behind such an override must be thoroughly documented, supported and approved by someone with appropriate authority. In addition to providing for

inherent risk scores, or internal control scores, trending indications can also be used, for example using the scale: increasing; stable; and decreasing.

Phase 3 - Arriving at the Net - Residual Risk

Once both the inherent risk and the internal control environment have each been established, the residual/net risk can be determined. Residual/net risk is the risk that remains after controls are applied against the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the internal controls.

The residual risk rating is used to assess whether the AML risks within the financial institutions are being adequately managed.

Using a standard three tier rating scale, the Residual Risk can be rated as High; Moderate or Low.

Residual Risk Determined: Example			
	Inherent Risk	Internal Controls	Residual Risk
Residual/ Net Risk	Low	85-100% Strong	Low
		75-84% Mod	Low
		Below 75% Weak	Mod
	Moderate	85-100% Strong	Low
		75-84% Mod	Mod
		below 75% Weak	High
High	High	85-100% Strong	Mod
		75-84% Mod	High
		Below 75% Weak	High

i) **Low Residual Risk** – The overall inherent risk of the bank/ business unit/business line, based on the clients, products/services, channels, geographies and other qualitative factors, is low and the mitigating internal controls are strong or moderate OR the inherent risk is moderate and internal controls are strong.

ii) **Moderate Residual Risk** – The overall inherent risk of the bank/ business unit/business line, based on the clients, products/services, channels, geographies and other qualitative factors, is moderate and the mitigat-

ing internal controls are weak OR the inherent risk is moderate and internal controls are moderate OR the inherent risk is high and the internal controls are strong.

iii) **High Residual Risk** – The overall inherent risk of the bank/ business unit/business line, based on the clients, products/services, channels, geographies and other qualitative factors, is high and the mitigating internal controls are moderate or weak OR the inherent risk is moderate and internal controls are weak.

Given the above methodology: i) A strong control environment can lower the residual AML risk in comparison to the inherent risk; ii) If the bank/ business unit/business line receives a high rating of inherent AML risk, it can never achieve a residual AML risk rating of low; and iii) In order to improve its residual AML risk in comparison to the inherent AML risk, the requirements for AML controls are commensurate with the results of the inherent AML risk assessment (i.e., stronger controls are required if the bank/ business unit/business line is assessed as having high inherent AML risk).

Reporting & Communication of Results

The results of the AML Risk Assessment, including the overall rating of the bank/ business unit/ business line as appropriate should be communicated by the legal/compliance/AML unit as appropriate to respective senior management, including with respect to the overall results for the firm to the firm's most senior management, the board of directors, internal audit and as requested to regulatory and supervisory authorities.

Across the industry, there has also been an increased focus on the levels of Operational Risk Capital held and the results of the Risk Assessment may be a useful input into the Operational Risk Capital calculation.

Note on Links to Customer Risk Rating Models

As financial institutions develop their Risk Assessment approaches consistently measuring risk in relation to established risk categories; for example geographies, products & services, channels, transactions and clients, these risk categories should also be taken into account and a model established to risk rate individual customer relationships.

Note on Links to Risk Based Approach

Once risks are identified, how to manage these should be a question for the financial institution provided as a minimum existing applicable laws and regulations are complied with. A financial institution will adopt a risk based approach to mitigate risks to match a net risk or risk appetite that it is satisfied with.

Other Approaches – Scenario Based Approach

As referred to above whilst it is increasingly common to use the “conventional/standard model” described above to approach Risk Assessment, other approaches are possible and valid. One such approach is the “Scenario Based Approach”.⁶

Whilst quantitative risk assessment methodologies have their place and form an important part of an AML Programme, we have certainly learnt from recent events that overreliance on historical data and analytical models may actually lead to overconfidence, recalling of course that many have a critical view of financial models and risk management processes and techniques, that failed to avoid the very unpleasant surprises, that have dominated the financial services industry leading up to, including and following the start of the global financial crises.

Still under any model we are not likely to avoid unpleasant surprises. We must nevertheless strive to understand the data we have and make careful observations so we may identify as many risks as possible. Quantitative models are an integral tool in promoting our understanding of the risks we face, and allow us to measure the residual or net risk after evaluating the strength of the control environment and to thereby seek to operate within acceptable risk limits. These quantitative risk models do have their limitations when it comes to considering very high-impact events. This is where scenario analysis can help as an additional risk management tool.

Scenario analysis follows a systematic process to create a set of possible events that may have a significant impact on a firm, for example tail risks amounting to stress testing. Scenarios are arrived at in different ways though usually by a team composed of key decision makers, experts, and/or stakeholder representatives. As they focus on areas of uncertainty and the potential for unexpected future tail events, scenarios provide a perspective not captured through analysis based on past data.

Scenario analysis has been used by both the public and private sectors for more than 25 years to manage risk and develop robust strategic plans in the face of an uncertain future. In certain industries, however, such as airlines, mining and nuclear power generation, operational losses can be truly catastrophic, involving deaths, injury and widespread destruction.

In contrast, in the finance industry the worst loss that can occur to a single firm may be its bankruptcy, as for example in the case of Barings or Lehman Brothers. However, financial sector stability and the ability for banks in a jurisdiction to be able to transact, settle and

clear transactions is of course a much bigger concern. In safety conscious industries, such as airlines, mining and nuclear power generation risk management is long established and well developed.

While the terminology is slightly different referring to safety management and not risk management, referring to ‘hazards’ rather than ‘risks’, and ‘containment’ rather than ‘mitigation’ its objectives are the same – the identification of potentially disastrous events and the reduction of the likelihood and impact of major events.

Scenario analysis has long been used by such industries and the tools and techniques used in such safety conscious industries are increasingly applicable to and being used also in the finance industry and, in particular, in connection with Operational Risk Management as defined by Basel II.

The use of scenario analysis is one of four approaches endorsed by the Basel Committee on Banking Supervision in its 2004 paper ‘Revised Framework for the International Convergence of Capital Measurement and Capital Standards’, which specified the definitive rules on capital charges for Operational Risk under Basel II (Basel 2004);⁷ alongside the use of internal loss data; relevant external loss data and bank-specific business environment and internal control factors and scenario analysis were each accepted together as tools to be used to qualify to use the Advanced Management Approaches (AMA), where Basel II requires that a bank’s internal measurement system must “reasonably estimate unexpected losses based on the combined use” of these four “fundamental elements”.

In their final proposal, the Basel Committee stressed the importance of ‘qualitative standards’ for banks that wish to use an AMA for management of their operational risks. However, other than urge that an Operational Risk Management (ORM) system must be “conceptually sound and implemented with integrity”, the Basel Committee gave few clues as to what such a ‘system’ might look like. Part of the reason for this was to allow banks to create an “internal model” that would better fit their unique operations, people and processes. Certainly an internally evolved system is likely to have a higher level of acceptance than a “one size fits all” prescription.

Scenario analysis and stress tests based on consideration of shock events and their possible repercussions can provide useful information for risk management purposes as well as regulators and other stakeholders. By careful selection, construction and analysis of scenarios unfolding over a period of time, a more holistic picture of the firm’s risk position can be created. Additionally, because such scenarios have at their heart a story-line, the com-

munication process with key stakeholders is less abstract than discussions focused on distributions, tails and other mathematical constructs.

The assessment of the relevant inherent risk facing a business can be determined by the nature of the business undertaken and the risks associated with that business, in other words – how that risk may actually occur given operations of the business. The inherent risk assessment can therefore be conducted at a scenario level. The scenarios represent ways in which an AML risk may crystallize. They are and can be considered to include significant long term events but can also be broader and more comprehensive.

The scenario approach allows a communication to occur in a language that will facilitate managements understanding of the risk itself and is likely to be compatible with common operational risk management approaches. The inherent risk assessment can be broken up into 3 parts: Part 1: Build the Scenarios; Part 2: Score the Scenarios; and Part 3: Determine the Inherent Risk.

Part 1 - Build the Scenarios

In this first part, a population of risks, or scenarios, possible events are created that may have an impact on a firm and/or may occur frequently. Most firms will already have a number of scenarios probably within the firms operational risk framework and these can be mapped to the AML related taxonomies, for example: for financial crime risks these may include separate assessments for AML, Sanctions, Anti-Bribery & Corruption. Examples of relevant scenarios are set out below:

Taxonomy	Scenario Examples
ABC	The risk that third parties that perform services for or on behalf of the bank or are associated with the bank pay bribes / confer undue advantage to public officials / PEPs in order to obtain or retain business or an advantage in the conduct of business for the bank.
AML	The risk that the bank on-boards a shell bank without identifying the increased money laundering threat and in contravention of regulation and policy.
Sanctions	The risk that the bank enters into or maintains business relationships or facilitates transactions with parties that are sanctioned entities.

See also Part 1, Section 2, Sub-section 2, Scenarios in P&S Risks

Part 2 – Score the Scenarios

In order to score the scenarios, a number of approaches can be taken. One example uses Impact and Relevance scoring models. The scoring model will determine whether the scenario has a low or high risk for frequency or relevance and a low or high risk for severity or impact, by applying a 1-4 rating scale for five categories for Relevance and four categories for Impact where 1 is low relevance and 4 is high relevance and 1 is low impact and 4 is high impact.

For **Relevance** factors the following can be considered:

- Regulatory Focus - assesses recent enforcement activity or regulatory interest in the area in the past 24 months.
- Business Activity - assesses whether the risk could crystallise given the day to day activities performed by the business
- Market and Product Profile - assesses the relevance of the risk given the products, markets and execution channels offered
- Client Profile - assesses the risk related to the client profile of the desk
- Personal Incentive - assess the likelihood of receipt of personal benefits which may incentivize behaviour that crystallised the risk

Where appropriate, these impact factors should also include the level of impact from a financial perspective such as regulator fines and penalties, costs of compliance and remediations as well as other civil and criminal fines and penalties.

For **Impact** factors the following can be considered:

- Regulatory Impact - assesses the level of impact from a regulatory perspective regulatory impact if the risk were to crystallise
- Reputational and Media Impact - assesses the potential reputational impact, including media coverage, if the risk were to crystallise

Once each scenario has a Relevance score and an Impact score these will be combined (for example RxI) to produce a gross risk figure for that scenario. For example if a scenario scored the maximum on both relevance for each factor (i.e. $4+4+4+4=16$) and impact for each factor ($4+4=8$) then combining the two figures (i.e. $16 \times 8 = 128$) will produce the maximum score possible, i.e. 128.

Part 3 - Determine the Inherent Risk

The total inherent risk score is derived by adding all inherent risk scenario scores and dividing by the number of scenarios. The total possible score (128xthe total number of scenarios) is then divided up into low,

Moderate and High possible outcomes, for example 80-100% of max is High: 40-80% of max is Medium and 0-40% of max is Low.

The inherent risk score for the bank, business unit or business line can then be used/taken and the internal control environment assessed and the residual risk determined as in the conventional/standard model above.

8. Risk Assessment and Risk Appetite

A Firm's AML Risk Assessment, should be designed by subject matter experts within the specialist unit responsible, for example, Compliance, AML, etc. and endorsed by the Firm's Senior Management. The same applies to other Risk Assessments, including Sanctions and Anti-Bribery and Corruption.

The result of the AML Risk Assessment will explain the current net AML risk being assumed by the Firm.

Senior management will need to determine whether the net risk is equal to the firm's risk appetite for AML Risk or whether the net risk exceeds the Firms risk appetite. In the latter case, measures will need to be agreed to be taken in order to either reduce the inherent risk or strengthen the control environment to ensure the net risk comes back into line with the firm's risk appetite. Alternatively, it may lead to discussion as to whether the firm's risk appetite is correctly positioned. The importance of senior management's involvement is especially illustrated here as a firm's risk appetite is a key influence upon its strategic goals and drivers.

A Firm's risk appetite may also be calibrated against other factors outside of the AML Risk Assessment Programme. For example, a set of scenarios and/or examples of risks/unwanted events which are relevant for the firm can be described and articulated to include a threshold impact amount, e.g. an acceptable level of loss per annum as a result of civil litigation.

Nevertheless, an example set of scenarios that could form part of a risk appetite evaluation and discussion with senior management could include defining expectations (risk appetite) and reporting on success and/or shortcomings (net or residual risk) with respect to the following risks: reputation, regulatory, civil liability and criminal liability.

a) Reputation Risk Damage - reputation damage can arise in numerous ways which affects the good reputation of a firm. A firm's reputation in this area is usually negatively affected by the announcement of a serious investigation into money laundering, usually in connection with client accounts and/or transactions, which

has or is likely you have a significant financial impact through regulatory, civil or criminal monetary fines and penalties. Reputation can also be negatively affected by existing and prospective clients, where negative allegations, including criminal allegations are made, for example, banking corrupt Politically Exposed Persons, facilitating terrorist finance transactions or dealings with questionable regimes, etc.

b) Regulatory Risk Damage - regulatory rules are constantly evolving and expectations increasing as to what a reasonable risk based AML programme looks like. Examination and testing experiences are also increasing in number, frequency, depth and intensity. The standard expected by regulators has largely shifted from accepting good or common practice to expecting the highest implemented standards as the norm. Matters once considered relatively minor, are increasingly considered material and matters once considered material requiring attention are increasingly considered material and requiring immediate attention. Costs for remediations and loopbacks, before fines can be substantial. Regulatory fines and penalties are being much more commonly levied for violations, often involving a number of regulatory agencies who take action for the same or similar issues. Part of this action is also likely to involve a commitment to undertake ongoing actions, including having a team appointed by regulators to be focused on ongoing monitoring of remediation of actions in situ at the firm.

c) Civil Liability Risk Damage - with civil class action lawsuits increasing and following investigations, fines or penalties levied in particular in connection with Sanctions matters, or terrorism finance cases as well as financial fraud liability for constructive trust, or civil action for failing to comply with a bank mandate, the possibility of legal damages being incurred is increasing.

d) Criminal Liability Risk Damage - whilst once very exceptional the prospect of criminal liability risks for AML weaknesses at a financial institution can no longer be discounted. The phrase "too big to jail" is one that grates amongst many who advocate criminal prosecutions and individual criminal liability as the only way to ensure satisfactory focus and full compliance by financial institutions with laws, regulations and expectations.

Whichever approach is chosen, and indeed both are possibly most useful operating in tandem then these must be endorsed by senior management, who will set and agree as well as monitor and revise as appropriate the AML risk appetite of the firm.

AML Programme

Anti-Money Laundering, which today often may include Sanctions Compliance, Anti Bribery and Corruption and Fraud Prevention Programmes have developed significantly over the last ten years or so. Starting as largely rules-based and focusing on automated screening and transaction reporting, involving few dedicated staff who undertook their responsibilities alongside other roles, it has evolved into an ever flexible risk-based operation, in the larger firms, employing hundreds of staff.

The following are the most important component parts for any successful Anti-Money Laundering (AML) programmes as expressly mandated, for example under S.352 USA Patriot Act 2001 which requires all financial institutions to establish AML programmes which, at a minimum, must include the following:

AML Programme - Core Elements	
1	Policies, procedures and controls
2	Designated compliance officer
3	Training programme for employees
4	Independent audit function to test the programme

Whilst each programme will include these elements the exact form of programme adopted by a financial institution will vary based on its own type of business, the size and complexity of its operations, the breadth and scope of its customer base, the number of employees, its risks and vulnerabilities to money laundering and the firm's resources.

Nevertheless, certain minimum standards must be a part of any adequate programme. For additional specifics relating to Sanctions Compliance, Anti Bribery & Corruption and Fraud Prevention see later in Part 1, Section 4 for details.

The programmes, whilst likely designed by the specialist Compliance AML unit, the business environment and the risk appetite needs to be set by senior management including the board and/or executive management. These bodies are responsible for the "tone from the top" defining the firm's values, behaviour and the culture that is needed to support an environment that puts sustainable, positive outcomes ahead of short-term gains. AML Risk Management may fit within existing governance arrangements where executive committees take responsibility for risk management in the first line and compli-

ance/AML units own the monitoring responsibilities for the control functions as the second line. Some firms may decide to establish dedicated AML risk committees to ensure AML risk receives a high level of focus.

First line of defence

As the first line of defence, management have responsibility for managing the ML/TF risk within their particular business area on an ongoing basis. The front office with the help of the infrastructure and support functions is considered to be the first line of defence in managing risk exposures for the firm. Whilst the front office is tasked with being a revenue generating section of the business, this needs to be balanced by the effective management of the risk the firm faces. Regulators have made it clear that they expect the front office to own and be held accountable for ML/TF risk within the business. As it is the front office that deals directly with or is accountable and responsible for the customer, the frontline needs to demonstrate that it is complying with ML/TF standards of due diligence and scrutiny. Management in the first line of defence have responsibility for monitoring the activities within their business and escalating where they do not.

It is important to clearly define the frontline responsibilities, as otherwise there may be an over-reliance on the second and third lines of defence. Where management in the front office do not recognise part of their role is risk management, this will inhibit front-to-back control and give rise to a weak culture and negative outcomes.

Second line of defence

The second line of defence is responsible for providing technical advice and monitoring the performance of the business against the ML/TF risk priorities set out by the board.

The AML Compliance control functions that form the second line should provide independent oversight, validation and verification of the management of risks by the business lines. They are also responsible for helping to define and challenge the risk framework, monitoring the risk profile of the business and ensuring that the business applies the framework consistently. The second line of defence monitors compliance with any directions and/or strategy set out by the board, investigates breaches, and reports directly to appropriate senior risk committees on the results of their work.

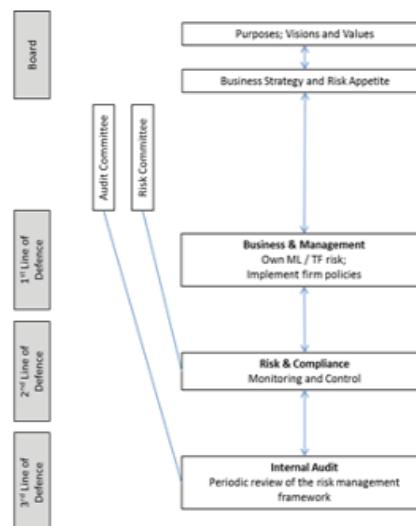
Third line of defence

The third line of defence is provided by an organisation's internal audit function. The internal audit function is responsible for providing independent assurance on the ML/TF risk-management framework, considering the

mechanisms in place within the first and second lines of defence and the extent to which these can be relied upon. It is independent of the business and the control functions within the second lines of defence.

Work performed at each level of the risk management framework may identify a need to revisit how ML/TF risk is managed and may also give rise to a need to reconsider the level of ML/TF risk the firm is exposed to. Communication from the Board on their expectations and demonstration of a tone from the top that holds individuals accountable for outcomes will help support a strong conduct risk culture throughout an organisation.

Three Lines of Defence Model for Effective Risk Management



1. Policies, Procedures and Controls

The starting point for any FI is to adopt a policy statement that clearly outlines the firm's policy against money laundering and its commitment to follow all applicable laws and regulations to ensure that its business is not used to facilitate money laundering. The policy statement should also make clear that all employees of the firm have a responsibility to follow the firm's written anti-money laundering procedures and controls, and to abide by all applicable laws and regulations involving anti-money laundering programmes. The policy statement also should discuss the consequences of not following these procedures.

Policies are usually drafted by the Compliance or specialist AML function. They are a representation of a firm's stance on managing its risks associated with legal and regulatory obligations whilst factoring in financial and reputational considerations. It can often be the case (see Sanctions section) where a firm's policy stance on an issue can go above and beyond legal and regulatory requirements and this is a firm's prerogative. Many firms with global operations look at their policies as establishing a global minimum standard and so policies must be adhered to except where local law/regulation requires a higher standard. This approach ensures that firms continue to undertake business always in accordance with the laws and regulation of the jurisdictions in which they operate.

Policies will usually reference other policies that should also be read alongside. Each policy will also refer to underlying procedures, which explain in more detail how a firm is actually able to comply with the policy. Policies and procedures must be clearly written, avoiding ambiguity and apply to all employees (including subsidiaries/related entities).

In drafting policies and procedures a firm may look to guidance provided by international bodies such as FATF, the Wolfsberg Group etc. but must ensure that the policies and procedures adequately direct a firm's AML approach and protect the firm from breaching its legal and regulatory obligations.

Policies should go through a rigorous development process and ensure that they receive the support of the senior management of a firm. Senior management, including the board, is responsible for establishing the 'tone from the top', instilling a culture of compliance, ensuring appropriate resources and expertise are in place to implement an effective programme; communicating regularly that commitment through internal and external channels; addressing serious matters with appropriate consequences for breaches; and, making ongoing assessments as to the competence, judgment and attitudes of senior management or persons in positions of supervisory control. In the absence of such a culture, compliance with policies is generally unsuccessful and as a result risks are not effectively managed.

The firm's procedures and controls should enable appropriate personnel to form a reasonable belief that they know the true identity of each customer; recognise suspicious customers and transactions; and require personnel to report suspicious or unusual activity to appropriate supervisory personnel, including senior management, and to regulatory and governmental authorities when appropriate. The firm's procedures and

controls should also ensure that the firm maintains an adequate audit trail to assist law enforcement agencies in any investigation. The key components of these policies, procedures and controls are as follows:

A. Customer Identification Programme

As part of its AML programme, a FI should adopt a written Customer Identification Programme (CIP). As part of the CIP it should specify the identifying information the firm will require from each customer. Although the type of identifying information a firm may require will vary based on, among other things, the nature of the firm's business and the type of customer, a firm must obtain certain minimum information prior to opening an account, for example for an individual customer, the customer's name, date of birth and a residential or business address and for non-natural persons, the customer's name and principal place of business, local office or other physical location. The CIP must also include risk-based procedures to verify the identity of each customer to the extent reasonable and practicable. Verification may occur within a reasonable time before or after the customer's account is opened. Accounts may be verified using documentary methods, non-documentary methods or a combination of both. The CIP, however, must describe under what circumstances the firm will use each of these methods. In addition, the CIP must identify situations where the firm will require additional verification based on the firm's risk assessment of the new account. The firm's CIP should also identify the documents that will be used for documentary verification.

A firm's procedures should also include a mechanism to identify potentially high-risk accounts in the account opening process. Although attempts to launder money or finance terrorism can come from numerous sources, firms should be aware that certain customer types, exposures to certain countries and usage of particular products and services may pose a greater risk (see Risk Assessment below).

The firm's CIP must also include procedures for determining whether a customer appears on any applicable lists of known or suspected terrorists or terrorist organisations issued by competent authorities

If a firm intends to reasonably rely on another financial institution, it must specify in its CIP when the firm will satisfy its obligations by relying upon another financial institution (including an affiliate).

B. Detection and SAR Filing

Another essential component of an effective anti-money laundering compliance programme is a set of systems

and procedures designed to detect and report suspicious activity. As with most components of a firm's compliance programme, the manner in which a firm monitors for suspicious activity will vary based on the firm's size and the nature of its business.

For some firms, appropriate manual monitoring of transactions in excess of a certain dollar amount may constitute acceptable review for suspicious transactions, while other firms may need to implement an automated monitoring process. Examples of suspicious transactions include those that have no business or apparent lawful purpose, are unusual for the customer, or lack any reasonable explanation. As discussed above, recognizing suspicious transactions requires familiarity with the firm's customers, including the customer's business practices, trading activity and patterns. What constitutes a suspicious transaction will vary depending on factors such as the identity of the customer and the nature of the particular transaction.

Since suspicious transactions may occur at the time an account is opened or at any time throughout the life of an account, firms must train appropriate staff to identify suspicious behaviour during the account opening process and monitor cash activity and trading activity in order to detect unusual transactions. Identifying suspicious activity may prove difficult and often requires subjective evaluation because the activity may be consistent with lawful transactions.

C. Risk Assessment

A firm must identify where financial crime may occur within the organisation. A risk assessment should be systematic and performed on an annual basis or as required. For more details on Risk Assessments see above. Whilst all aspects of financial crime should be subject to risk assessment in order to assess a firm's inherent and net risk of its activities, its products and services being abused and the risks posed by its customers. Risk Assessments may be carried out for major business divisions, business units or lines as deemed appropriate.

The Risk Assessment may also be leveraged to risk rate the firm's customers and used to determine the approach to be taken in terms of the required due diligence and monitoring will be fixed. A basic level of due diligence is required for those clients determined to pose the lowest risk, with an increased or enhanced level of due diligence required for those clients determined to pose a higher risk as well as other control measures that will need to be enhanced. Various factors will be taken into account when deciding the appropriate risk category for a client. The following table below highlights the main areas of focus which together via an appropri-

ate scoring model, appropriately weighted can be used to risk rate clients.

Clients' Risk - Checklist

1. Clients' Factors

- Entity risks, duration/length of relationship, Negative Media Reputation Risks, Industry Risks, Profession/Activity Risks

2. Products & Services Factors

- Line of business risks and utilisation of increased risk products and services

3. Channels Factors

- Account origination and servicing solicited/unsolicited; face-to-face or non-face-to-face

4. Country Factors

- Increased risk countries and in country hotspots and regional hotspots

5. Transactions Factors

- Unusual and/or suspicious transactions alerts, investigations and SAR filings

go much further. These restrictions can stem from legal or regulatory drivers or be as a result of a reputational risk assessment of the risks posed in a particular case.

For more details see Part 1, Section 2, Sub-section 2, Customer Risks; Sub-section 3, Products and Services Risks (including Channels Risks) and Sub-section 4, Country Risks above, as well as Risk Assessment above in Risk Assessment, Part 1, Section 4.

D. Monitoring and Controls

A firm must implement controls that are designed to manage the risks that it faces. A compliance programme can benefit from a written monitoring and control plan that identifies what should be monitored and controlled, when and by whom. Firms generally apply three lines of defence in AML Compliance. The first line of defence is with the front office, for example in relation to day to day client onboarding and ongoing monitoring. It is essential that the front office understand their responsibilities, rather than seeing AML as 'just a compliance issue'. The second line of defence is with the Compliance or AML function that may control or sample check for example, client KYC files, transaction due diligence files, payment review decisions, screening of records, etc. Such functions may also undertake the monitoring described in an annual monitoring and control plan which seeks to report back on the most significant risk areas. Regular monitoring across different risk areas can provide indication of systemic weakness in controls as well as be used for predicting horizon risks. Reports should be communicated to management who should be in a position to reprioritise strategy and resources as required. This process involves continuous review and improvement, as indeed do all parts of a risk based AML Programme. The third line of defence is played by internal audit who evaluate the risks and controls and inform senior management reporting to the Board of Directors Audit Committee. In many countries, external auditors may also play an important role in evaluating Banks' internal controls and procedures.

Ensuring client due diligence is correct and appropriate is an important control. The client risk category assigned to a client will determine the frequency of monitoring the client is subjected to. For example, a higher risk client will face more regular reviews of its client due diligence information and would also be subject to enhanced monitoring of transaction activity, which can be based on either or both of frequency of monitoring or transactional volume. At each review, a firm has an opportunity and a duty to ensure KYC information is up to date. Doing this also allows screening of the KYC information against sanctions lists, for example. The higher the risk rating for a client, the more monitor-

ing and controls they are subjected to. This ensures the firm continues to meet legal and regulatory obligations, and to protect its reputation, whilst at the same time ensuring it is easier for lower risk clients in terms of the conditions associated with managing their relationship. Sampling of client files or transactional activity is commonly used as way of indicating whether controls for onboarding clients are operating appropriately.

Tools used to conduct controls should be periodically tested, including transaction filters and their data feeds. Sometimes this testing requires IT expertise, and sometimes testing can be conducted by Compliance, via sampling.

Controls and monitoring can be ‘prevention’ based or ‘detection’ based. Preventative controls aimed at putting a stop to risks from manifesting are usually hardwired into systems used to manage risk, for example, not allowing approval of a gift without Compliance providing consent. In this example, detective controls would aim to identify those instances where such approval was not provided. The combination of both of these types of controls would be targeted at each risk identified, with risks considered to be greater receiving the most resources to mitigate them.

Controls need to be continually assessed for effectiveness. An undetected control failure can result in breach of law or regulation, not to mention the subsequent reputational impact in the event of public enforcement action. No good programme remains static. Industry standards change, as do regulator expectations.

E. MIS/Reporting

Various controls in place at a firm can be configured to generate metrics. Metrics can be used by an AML professional to monitor the ways in which its client profiles or business focus is changing, as well as to highlight areas where there may be control weaknesses. Such metrics should be made available to senior management, with issue action tracking used to close any outstanding issues as well as regular reporting on the status and effectiveness of the overall programme.

F. Record Keeping

A firm should have clear record keeping policies regarding its AML programme as well as evidence around clients and transactions. As far as clients and transactions are concerned a firm must maintain records for at least five years after accounts are closed or transactions undertaken. Firms should also be prepared to provide programme information to their regulators and, on occasion, to local law enforcement. Decisions made must be recorded and those records must be kept in line with

firm policy and legal obligation. AML professionals in particular must be in a position to justify the actions they took in any given scenario, with that decision having followed prescribed procedure. The importance of keeping client-related documentation safe and retrievable is also clear, with firms having been subject to enforcement action for not doing so. A firm’s systems and controls should be interwoven with the concepts of record keeping and retrieval. Keeping client due diligence information up to date is also an ideal way of remaining well placed to meet legal and regulatory requirements. A search for a particular client that has been requested by a regulator, for example, could result in a client being missed if the information held on them is out of date or has been recorded incorrectly. Maintaining accurate records also allows firms to target business opportunities more effectively if they know their clients well.

2. Designated Compliance Officer

In most jurisdictions it is a requirement that a firm designate an individual or individuals to oversee the AML programme, including the firm’s CIP operating separately from the front office functions. This person may be the compliance officer that is responsible for other compliance areas of the firm or a dedicated AML officer, who in either case should have AML related expertise and have the ability to explain risks to senior management, the front office, IT and operations personnel.

A firm must provide its compliance officer with sufficient authority and resources to effectively implement the firm’s AML programme. Among other duties with respect to the firm’s CIP and suspicious activity reporting, this person should:

- a) receive reports of suspicious activity from firm personnel;
- b) gather all relevant business information to evaluate and investigate suspicious activity; and
- c) determine whether the activity warrants reporting to senior management, and/or to the appropriate authorities.

The person responsible for overseeing the AML procedures should not be the same employee responsible for the functional areas where money laundering activity may occur.

While the AML officer directs the AML programme, the programme should make clear that compliance is the responsibility of all employees. The “front office” of any business should be primarily responsible for the business it brings into a company, and is often in the best position to collect the client information needed to satisfy KYC and due diligence requirements and to

determine whether transactions are legitimate. It is vital that the function has a relationship with external bodies and other competitors to benchmark and leverage from industry best practice.

These relationships could include:

- a) Law enforcement agencies
- b) Government agencies
- c) Trade & industry bodies
- d) Peer firms/competitors

3. Training Programme

Another important component of an AML Programme is the requirement to provide ongoing education and training for all relevant personnel. This training programme should be conducted at least at regular intervals and include training on the firm’s policies and procedures and the relevant laws and regulations. Staff in different roles will have differing training needs and a firm must identify what these needs are and target staff with appropriate training in order to carry out their duties in accordance with policy, law and regulation. This can mean that the majority of staff receive a training module which is generic, while staff with greater exposure to financial crime receiving an enhanced module, maybe with a test. Staff can be split into a number of different categories, receive training by different means (for example, computer-based or face-to-face etc.) and also receive training at differing frequencies depending on the risks they face. Local language requirements should be considered to ensure the audience understands the key messages and requirements.

Effective training modules should also include the use of case studies, highlighting red flags, as well as past enforcement cases. Apart from this being a way to show an individual undertaking the training how detecting financial crime applies to them, it is a great way of avoiding the monotony of imparting the obligations placed on staff.

Training must receive the support of senior management at a firm. The ‘tone from the top’ should emphasise how important training is to a firm and mandate its completion. The consequences of non-completion should also be made clear.

It is one thing to provide training and another to ensure that training is effective. A training module can be accompanied by a test that must be passed with an escalation procedure for those unable to pass after a few attempts. The training material must also be reviewed regularly to ensure it continues to reflect risks as they stand and the direction of the business.

Whichever approach is taken by a firm, it must be able to defend its position. Additionally, training is one part of staff education. A firm should also maintain staff awareness of the risks they face and their responsibilities. This can be via a number of means, for example, poster campaigns, regular compliance releases detailing changes to risks or interesting cases, etc.

Firms should maintain records to evidence the training provided to and received by staff.

4. Independent Testing

Independent testing of the adequacy of AML compliance programmes is essential. Firms should conduct regular independent testing. A firm may carry out independent testing through its own personnel (such as an internal audit staff) or others who do not perform or oversee AML functions. In either circumstance, the audit function should test all affected areas to ensure that personnel understand and are complying with the AML policies and procedures and that these policies and procedures are adequate. The results of any audit should be documented and reported to the firm’s senior management or an internal audit committee or department, and follow up should be done to ensure that any deficiencies in the firm’s anti-money laundering programme are addressed and corrected. External auditors may also be appointed in certain circumstances to evaluate a firm’s AML programme, however, they would normally seek to review any internal audits undertaken as part of their review.

Sanctions Programme

Sanctions are any measure or restriction taken by one or more countries (or their respective government agencies) or international organisations which are aimed at restricting dealings of any kind with or involving another country, specific persons, legal entities, organisations or goods (sanctioned parties). Whilst sanctions have been in place for a number of years, it was not until 9/11 that sanctions regimes were brought to the forefront of firms' attention. Funds are needed to commit any terrorist act and the US Government in particular sought to ensure that US firms or US persons were not permitted to engage in any kind of business activity with or provide any goods or services to sanctioned parties. Other developed countries also increased the requirements of their sanctions programmes after this event. With increased legislation and regulation, firms had to develop sanctions compliance programmes.

There are some issues of global concern that are addressed by sanctions - human rights, genocide, and weapons proliferation, preservation of the integrity of the financial system, corruption and global terrorist financing. Sanctions could, however, be a means by which governments can extend their foreign policy agenda. Whatever the reasons, increasing enforcement action by authorities has meant firms have had to make significant enhancements to their sanctions programmes. As breaching sanctions is usually a strict liability offence, there is an increased focus on a firm having adequate systems and controls to guard against breaches. Stiff penalties, both in terms of monetary fines and imprisonment can befall any individual or entity that has breached sanctions.

Restrictions imposed could include travel bans, trade and arms embargoes, asset freezes, etc. All of these types of measures are aimed at restricting the extent to which the financial services industry is able to provide products or services to individuals and entities thought to be supporting regimes or undertaking activities which are not considered acceptable.

Sanctions Programme - Core Elements	
1	policies, procedures and controls
2	designated compliance officer
3	training programme for employees
4	independent audit function to test the programme
Source: Author	

Whilst compliance with sanctions is absolute, firms are permitted to take a risk based approach to compliance. In doing so, a firm must be prepared to defend its approach. A firm's approach should include the following core elements.

1. Policies, Procedures and Controls

As with an AML programme, a firm must decide its own interpretation of legal, regulatory and reputational risk and arrive at a policy stance. It has been argued that for sanctions and AML that firms have a corporate social responsibility in terms of preventing breaches of law and regulation. As such, firms should consider a policy statement in complying with sanctions from specified sources as part of its code of conduct in addition to developing a robust sanctions policy.

A. Sanctions Compliance Policy

The first step in constructing the sanctions policy is to define what those restrictions are meant to accomplish. Businesses must comply with the laws of jurisdictions where they do business. Most are concerned about protecting their reputation. Many are concerned with acting responsibly on key issues. There might not be global consensus on what it means to "do the right thing" regarding sanctions compliance, as one country's embargo might not be embraced by another.

The types or risks which should be addressed in sanctions policies include:

- a) Applicability of sanctions lists
- b) Sanctioned countries/governments/regimes
- c) Screening of new and existing clients
- d) Screening of transactions
- e) Prohibited transactions
- f) Pre-approvals and escalation of issues
- g) Freezing/blocking of assets and reporting

Global companies often incorporate into their policies measures imposed by the UN, EU and US to stay on the right side of major issues. One reason for including the US restrictions globally is the list of large penalties described in Part 2, Section 8, Enforcement Cases. Several non-US financial institutions have tried to steer clear of US sanctions laws and failed because they did not employ a global approach. US jurisdiction can be triggered by the involvement of a US person anywhere in the world, involvement of a US system or platform, or involvement of a non-US person who has caused US persons to violate US sanctions law. It might not be easy for every company to administer a procedure for employees who are "US persons" to recuse themselves from activity involving sanctioned countries, particularly if those employees are senior executives in control of busi-

ness lines and operations with a global reach.

In designing a sanctions policy, it is also best to think ahead. Effective sanctions programmes should be forward thinking to anticipate sudden sanctions events that could prove disruptive and costly if businesses are caught unaware. A forward-looking list of sanctions restrictions can be created to enable escalations to subject matter experts. That list may proactively exceed strict legal requirements to avoid accidental contact with a sanctioned entity's behaviour.

A firm's sanctions policies and procedures should also require risk based screening of transactions against sanctions lists – particularly those sanctions lists applicable in the countries where it does business and relevant to the firm's sanctions policy. Financial transactions sanctions screening normally occurs in "real time" or as the transactions occur. Identifying a sanctioned transaction after it is processed is too late in that it fails to prevent funds from reaching or otherwise benefitting sanctioned parties. Real time review of sanctions hits can be more resource intensive than the historical monitoring of transactions for suspicious activity. Financial institutions generally automate electronic funds transfer screening and employ smart filters able to detect sanctioned country locations and name variations. Regulators of financial institutions generally require written procedures for the handling of payment filter "hits".

B. Detection and SAR Filing

In the event that employees identify activity which may be in breach of sanctions, either manually or by using an automated system, they must escalate in accordance with policy. Such escalations are usually to Compliance who will undertake an investigation and decide the necessary action. Internally, appropriate action could range from conducting enhanced monitoring on an account or client to the extreme of terminating a client relationship. Externally, it could mean making a report to a regulator where it is believed that a sanctions requirement has been breached or if there is a specific requirement that a payment should be blocked or rejected. Additionally, in the course of the investigation, Compliance officers should also consider whether any activity identified should also be the subject of a SAR. Whilst not all SARs are likely to have elements related to sanctions, sanction investigations should be considered for suspicious activity.

C. Risk Assessment

As with AML risk assessments, it is practical to assign an initial inherent risk rating, consider mitigating controls, and then assign a residual risk rating. The fact that sanctions risk is not synonymous with AML risk makes it

difficult to apply the AML methodology to a sanctions risk assessment. An AML risk assessment might use a quantitative approach, such as assigning risk numbers to client types and weighing them against dollar volumes, but this might not be as useful for sanctions.

Another approach to sanctions risk is to identify ways the company's activities could result in a benefit to a sanctioned party. Does a business make available anything of value – including services, merchandise, payments, loans or credit to persons other than vetted clients? The following under D. Monitoring and controls below include a number of increased risks of products, services, customer types related to the financial industry that may potentially be considered as part of a Sanctions Risk Assesment. For more specific details see Risk Assessment above.

Major Sanctions Risks	
i)	International fund transfers
ii)	Correspondent banking
iii)	International commercial shipping lines or freight forwarders operating via transit routes known for drugs, arms or sanctioned parties
iv)	Energy and commodities companies operating in sanctioned regions
v)	Money service business
vi)	Charities

However, no single group of industries are categorically high risk for sanctions. Countries require all nationals to comply with sanctions restrictions. Therefore, a violation can occur in just about any industry. Moreover, while some sanctioned countries derive revenues from a particular sector - energy, for example - not all energy companies deal with sanctioned parties.

D. Monitoring and Controls

Weaknesses in a firm's sanctions compliance programme are usually identified either in relation to the screening of payments or a firm's client base for sanctioned parties. Most firms make use of an external data provider for up to date sanctions lists to ensure it continues to be in compliance with legal requirements. The controls that are put in place will depend largely on the size, business nature, structure and geographical footprint of the organisation. The controls that are in place must be risk based and targeted. Some of the high risk areas identified above have been selected to illustrate this:

(i) International fund transfers

Sanctions regimes will contain restrictions on payments

to sanctioned individuals, entities and regimes and also in relation to certain types of goods, for example, arms, US origin goods to specified countries, etc. The international transfer of funds has been a key way for those trying to evade sanctions to send their money internationally without being detected and stopped.

Sanctioned parties excluded from international commerce will of course turn to agents and front companies to access financial systems without detection. Therefore, it is imperative that a company knows its customers, partners and counterparties or other third parties who act on a firm's behalf, and that they are all screened against relevant sanctions lists. Additionally, a firm providing electronic funds transfers to its clients must ensure that they comply with international standards for those transfers, for example, ensuring that payments are not processed without suitable and accurate remitter and beneficiary information, or that payments are flagged if they are potential breaches of sanctions requirements. The importance of ongoing due diligence and reviews is imperative here.

(ii) Correspondent Banking

Whilst correspondent banking is a key way of providing access to a certain jurisdiction's financial system without being present in that jurisdiction, there are many risks associated with this activity. Providing such services allows the movement of funds which may be subject to abuse and as such increased controls are required in this area. Those controls start right from the onboarding stage. As previously discussed, if correspondent banking clients are from a jurisdiction that is known to carry higher AML, sanctions or bribery and corruption risks then firms must ensure they have collected enough due diligence to become comfortable with the relationship. This includes understanding the correspondent banking client's customer base. Certain customers will be of especially high risk and these must be identified. For a firm providing correspondent banking services to a client, it is often interpreted to be a sign of that firm vouching for their client. Correspondent banking relationships can be identified from payment messages and firms should consider the reputational risk associated with a client prior to offering them this service. Commensurate monitoring of their activities must take place. Such monitoring can be based on a transaction volumes but should be enhanced with a focus on things like patterns of payments, recipients, currencies, jurisdictions, etc.

Those wishing to evade sanctions can create fictitious front companies to undertake transactions and there must be controls in place which seek to identify such companies. Monitoring suspicious activity is a key way of doing this. When it is identified, the suspicious activ-

ity should be investigated and reported where necessary. Transaction information should be analysed to ensure that there are no sanctions concerns about any payments that are processed and that firms are not being used as a conduit to divert funds to sanctioned individuals, entities and regimes.

Staff need to be made aware of the types of activity that could indicate attempts to evade sanctions and understand that additional due diligence may be appropriate before processing payments.

(iii) International commercial shipping lines or freight forwarders operating via transit routes known for drugs, arms or sanctioned parties

The shipping industry carries a risk of contravening international sanctions primarily due to the ways in which it is possible for entities to disguise/conceal the identities of vessel owners, goods carried and origin/destination of goods. Firms will usually class the shipping industry as one of the higher risk industries simply because of this and must, therefore, perform due diligence to know with whom they are contracting. Failure to conduct appropriate due diligence on shippers and freight forwarders as well as all of the parties that may be involved in a trade finance transaction could be subject to sanctions violations for having facilitated activities that contravene sanctions laws.

There are a number of ways in which sanctions risks could arise: a ship could be controlled by ownership or charter agreement to provide services to a sanctioned party; or the use of a ship, controlled by ownership or charter agreement, to provide shipping services for the purpose of supplying goods to be used in contravention of sanctions regulations.

At the client onboarding stage and as part of a regular review, a firm must ensure it has systems and controls in place to identify the involvement of sanctioned parties, including understanding the intended business. If it is known that a particular commodity or shipping route will be used, for example, and that route has increased sanctions risks then this will help a firm determine what if any legal and/or reputational risks exist to permit the establishment of the relationship or transaction.

When first engaging in business, a firm may choose to include certain representations and warranties in contracts to secure some protection. However, representations and warranties in a contract should never be a substitute for due diligence including how a shipping line ensures it complies with international sanctions, how it screens vessels, or how it ensures goods are not being transported via sanctioned regions etc. Whilst the

shipping industry in certain regions may be reluctant to undertake these types of controls, firms should nevertheless insist that such controls are present before they conduct business with such shippers.

Depending on the nature of a firm's business activity, if they are involved in providing trade finance support to their clients, there is an expectation that as part of carrying out a transaction or deal they are inspecting documents such as letters of credit, bills of lading, etc. These documents may assist a firm in identifying any potential sanctions risks that may exist.

(iv) Energy and Commodities companies operating in sanctioned regions

A number of well known and large energy companies operate in or around sanctioned regions as do commodities companies. Some of these companies carry licenses which have been granted by government authorities and others are usually careful to ensure they do not breach international sanctions by restricting the type of business they undertake. Some sanctions regimes are very specific to certain types of energy from certain jurisdictions, for example petroleum based products from Iran.

When such companies approach a firm for business, the firm should ensure it understands fully the nature of that customer's business. Enhanced due diligence at the start should allow the early identification of issues and as stated above, can impact the extent and scope of sanctions representations and warranties and other controls that could be appropriate. A firm should monitor the transactions and behaviour of entities like those involved in the energy and commodity sector given the higher risk these entities represent including requiring more detail about the extent of the business, and more frequent site visits, for example, to conduct risk assessments. Thus, a firm's approach should be to ensure the risks in onboarding a customer are sufficiently addressed and that a periodic review is conducted to ensure that the risks have not changed.

(v) Money Service Businesses

Firms offering products or services to Money Service Businesses (MSBs) should be aware of the inherent money laundering risks associated with such activity. The fact that it is possible to conceal the identity of underlying remitters or receivers of payments is one of the reasons why this is a high risk industry for both AML and sanctions. A firm offering products or services to a MSB should be aware of how and from where the MSB generates its revenues. Even an indirect connection to sanctioned parties can create legal exposure. The revenues derived from a sanctioned region might be a small percentage of a company's overall revenue, but may pro-

duce a clear benefit for sanctioned parties. A UK-based, regulated MSB will carry different risks to one located in the Middle East, for example, and therefore, require different due diligence and ongoing monitoring of the account activity.

As mentioned at the beginning of this chapter, sanctions restrictions could be aimed at particular regimes. It is thought that economic sanctions, that is depriving the regime from access to the financial markets, can be used to persuade the regime to amend its ways. In reality, amending its ways is the last resort for such regimes. Instead, rogue regimes will usually concoct ways to evade sanctions, such as creating fictitious companies and complex structures aimed to conceal the identity of the true beneficial owner(s). Such regimes can then use these fictitious companies to send money through MSBs. Given the significant risks posed by MSBs and the types of business they conduct, some firms may decide that appropriately that MSBs are too risky to have as a client and prohibit the establishment of MSB relationships altogether. Where a firm decides to establish such relationships, it should do so only after conducting appropriate due diligence, obtaining senior management approval and subjecting the MSB to regular and robust monitoring to ensure transactions are analysed for suspicious activity and that the risks have not changed.

(vi) Charities

Whilst charitable giving is to be fully supported, terrorist groups have benefitted and so care needs to be taken with respect to charity customers particularly ones operating in or around sanctioned countries.

E. MIS/Reporting

Firms should operate a robust reporting framework as part of their sanctions programme, which allows senior management to be made aware of how well the controls in the programme are working. Reporting on how sanctions alerts are being cleared by a dedicated team, the number of payments/messages that are screened and released, the number of customers that are screened, as well as the number of payment messages or clients that are reported to authorities are some of the ways in which a programme's effectiveness can be assessed through reporting. Such reports will also provide a view as to how sanctions risks are changing, that is increasing, stable, or decreasing. Regular reporting can also help to determine if policies need to be changed or supplemented.

Firms with an international presence may also seek to monitor whether certain international offices are undertaking business with certain regions or industries that are known to be at higher risk of sanctions risks or

violations. Capturing this kind of data allows a firm to take a wholesale view as to whether sanctions risks are being assessed consistently across the firm. Sanctions restrictions are constantly changing. Therefore, it is important that a firm keep abreast of new sanctions regulations and key enforcement actions and assess whether its internal processes and controls are sufficient to demonstrate it has in place a robust sanctions compliance programme.

F. Record Keeping

Whilst keeping records is a legal requirement, it is also an expectation of regulators and government agencies. The plethora of enforcement actions involving sanctions violations committed by a firm over a period of time reminds us that maintaining transaction details including details regarding sanctions risk reviews is a critical part of protecting a firm in the event of a sanctions issue. Indeed, documenting the rationale for processing or rejecting a payment, engaging in a transaction or onboarding a client where sanctions risks are identified could mean the difference between a sanctions fine and no action taken by a regulator or government agency. Firms should ensure there is periodic communication and training regarding the importance of documenting and recording the actions taken or decisions made about a client or a transaction particularly when such action involves a potential sanctions issue.

2. Designated Compliance Officer

A sanctions compliance programme requires a dedicated officer operating separately from the front office functions. The officer should oversee guidance, training, controls, and monitoring of those controls. The sanctions officer should have sanctions-related expertise and the ability to explain risks to senior management, the front office, IT and operations personnel, as well as externally to regulators and law enforcement. Whilst the sanctions officer directs the sanctions programme, it should be communicated that an effective sanctions compliance programme is the responsibility of all employees. The “front office” of any business, which is primarily responsible for the business it brings into a company, and is often in the best position to collect the client information, details about a client’s business and the purpose of the relationship which is needed to satisfy KYC and due diligence requirements. It is also important that operations personnel to understand how sanctions requirements might affect the transactions systems and flows they manage. Thus, these groups will require guidance from compliance regarding sanctions risks that may arise in processing transactions or managing systems.

3. Training Programme

Developing and providing targeted training to staff based on their roles and responsibilities is essential to ensure employees are equipped to address and manage sanctions risk. Once training needs have been identified and material developed, training should be conducted on a regular basis. For those roles that carry a higher risk of exposure to sanctions, ordinarily firms should ensure that sanctions training be accompanied by a test to demonstrate understanding and knowledge gained from such training. This should also include sanctions awareness communications when important regulatory or legal changes occur. Finally, the frequency of training will differ according to the sanctions exposure faced by a particular group. Identifying training needs on an annual basis will help to demonstrate that a firm understands and communicates emerging risks and implements the appropriate controls to mitigate that risk.

4. Independent Testing

All aspects of a sanctions programme should be subject to independent testing. Whether internally or externally driven, such tests should aim to provide some assurance that processes and controls are operating effectively to mitigate the likelihood of violating sanctions laws. Compliance departments’ own testing should also be verified independently. This includes at the minimum testing the effectiveness of, reporting, training, payments processing and client and deal due diligence. The frequency of testing should be determined using a risk based approach. Whilst not all aspects of a programme need to be tested at the same time, all aspects should be subject to testing on a periodic basis. Choosing which aspects to test may be driven by whether any MIS reporting has highlighted any breaches or trends, or, for example, whether there has been an increase of accounts opened in a higher risk jurisdiction. Whichever area is targeted the rationale for the decision should be recorded

Anti Bribery & Corruption Programme

Whilst third party corruption, i.e. bank customers, is covered by a financial institutions AML Programme, the financial institution must also seek to prevent its own employees from any involvement in bribery or corruption both on the supply side or on the demand side. An effective Anti Bribery & Corruption (ABC) Programme is essential, both to protect the firm from any involvement in bribery or corruption and as a defence in case any individual cases or allegations arise.

There has been a lot of commentary over the last few years, particularly from Bank regulators, law enforcement agencies, international bodies and NGOs as to what constitutes an effective ABC Programme with various papers and guidance being issued.

Of course as with any other type of compliance programme, the type of programme implemented to prevent bribery and corruption will depend on the size, business nature and structure of the organisation. It should also include the following core elements but tailored towards ABC:

ABC Programme - Core Elements	
1	Policies, procedures and controls
2	Designated compliance officer
3	Training programme for employees
4	Independent audit function to test the programme

Source: Author

1. Policies, Procedures & Controls;

The starting point for any financial institution is to adopt a policy statement that clearly outlines the firm’s policy against bribery and corruption.

A. Code of Conduct / Specific Policies

Whilst a firm wide Policy should spell out in detail the firm’s approach, the headline approach should be included succinctly in a firm’s overall Code of Conduct, where an unequivocal zero tolerance stance against bribery and corruption by the firm’s employees and those acting on the firm’s behalf should be made clear.

Beyond this clear articulation of a firm’s overall position, a group wide high level Policy will include greater detail but specific Policies will also need to be issued, with supporting procedures and controls. These areas for

specific attention should be formulated and updated following the completion of an appropriate risk assessment exercise.

B. Detection and SAR Filing

In the event that suspicions arise of employee behaviour which indicates the giving or receiving of a bribe or other form of corruption, the event should be treated very much in the same way as a third party case and considered for SAR filing and other possible notifications (or ‘self disclosure’) to the authorities as well as pursuing the investigation internally, which will be normal in the circumstances.

C. Risk Assessment

As with AML risk assessments, it may make sense to assign an initial inherent risk rating, consider mitigating controls and then assign a residual risk rating. As with sanctions risk, ABC risk is however not synonymous with AML risk and so it is difficult to apply the AML methodology to an ABC risk assessment. A firm should therefore identify where specific ABC risks may occur within the organisation. It is likely that in most firms the following areas will require consideration and may be considered as having increased risks:

Major ABC Risks	
i)	Dealing with public officials and particularly ones who would also qualify as PEPs
ii)	Dealing with persons from jurisdictions or in industries with inherent elevated risks of corruption
iii)	Gifts, hospitality, entertainment and travel
iv)	Political contributions
v)	Charitable donations and sponsorships
vi)	Facilitation payments (which many firms will want to prohibit)
vii)	Books and records
viii)	Solicitations
ix)	Offers of employment, internships and the like
x)	Deals with third parties, agents and intermediaries

D. Monitoring & Controls

ABC controls largely rely on staff escalating issues when they should and in a timely manner. Whilst there can be automated systems in place, staff will still need to know how to identify bribery or corruption using these systems.

(i) Public Officials

In managing the risks associated with a public official, such a term first needs a clear definition articulated within the ABC Policy. Unlike for PEPs where the definition is enshrined within legislation, for public officials, industry guidance can be relied upon but is quite broad. Government entities are usually regarded as public officials and by implication, employees of that government entity would also be considered to be a public official when acting in their professional capacity. In the identification of these public officials, firms should also have the ability to confirm whether or not they qualify as PEPs. Whilst an individual may be a public official without being a PEP, a PEP will always be a public official.

The risks associated with a public official are that they are, by virtue of their position within a jurisdiction's government/government entity, political party or judicial body, susceptible to the receipt of bribes. Firms should ensure that there is a process for identifying the presence of a public official in any business dealings and that any transfer of any kind of value is subject to pre-approval, normally by Compliance. So, ordinarily the giving or receiving of gifts, entertainment, etc. in relation to public officials will be monitored for any breaches of policy.

(ii) Dealing with persons from jurisdictions or in industries with inherent elevated risks of corruption

A firm's approach to managing AML will have increased monitoring and controls in place in general for higher risk clients. Beneficial owners, industries and jurisdictions will all form a part of the risk considerations to determine which risk category a client will belong to. In accordance with a firm's country risk model, jurisdictions are risk rated and one of the factors taken into account is bribery and corruption risk. The susceptibility of individuals, including public officials, to bribes and corruption may be higher in some jurisdictions than others. A firm's country risk model may place reliance on Transparency International's Corruption Perceptions Index, for example, which will assist in identifying jurisdictions where there is an increased risk of bribery or corruption.

Certain industries also carry a higher risk of bribery and corruption. Examples include extractive industries, defence and aerospace industries. If a client relationship involves a high risk industry then the overall controls applied to that relationship will increase. More in-depth checks when the client's due diligence information is reviewed will seek to continue to identify the involvement of any individuals, entities or industries which present a higher bribery and corruption risk and monitor such involvement on an ongoing basis.

(iii) Gifts, hospitality, entertainment and travel

One of the key ways of trying to disguise the giving/receipt of bribes is to pass them off as a gift, hospitality, entertainment or travel. Whilst these can form part of the normal course of business, a firm must have controls in place to ensure that the transfer of any value is above board. A client relationship manager may choose to provide a potential or actual client with some form of inducement to engage in business or a client themselves may provide such an inducement to secure favourable business terms. A firm needs to have registers in place which record precise details about any gifts, entertainment, hospitality or travel. These registers should then be sample checked on a risk based approach to ensure that the transfer of any value is conducted in accordance with policy. Guidance should be provided to all staff to ensure there are no ambiguities in their responsibilities.

(iv) Political contributions;

All political regimes need to raise funds in some manner. Corrupt regimes may choose to directly request or strongly intimate that a political contribution is required in order to secure favourable business terms. There should be a mechanism in place for recording all donations of this kind with sample based checking to ensure the donations had the appropriate pre-approvals.

(v) Charitable donations and sponsorships;

In a similar way, clients involved in charities may infer or request a donation or sponsorship of an event in order to secure business. Charities are also at a higher risk of corruption and money laundering and so increased vigilance is especially required. Pre-approval processes, together with regular checks to ensure processes are being followed will allow better management of the risk of bribery or corruption.

(vi) Facilitation payments

Facilitation payments (also known as "grease payments") are small payments made to secure or expedite the performance of routine or necessary action to which the payer is legally or otherwise entitled. Many firms will want a complete prohibition on all facilitation payments in order to comply with bribery and corruption laws. However, in some jurisdictions or regions, these types of payment are commonly accepted as part of the fabric of commerce. A firm could use the kinds of registers mentioned above to spot facilitation payments, though this can be challenging and relies on staff to correctly identify and report any direct or indirect requests for such payments. Where facilitation payments are prohibited, staff need to be made aware of this, especially in those regions where they are commonplace, as well as how to report such instances.

(vii) Books and records

The system of internal controls must be designed to ensure reasonably fair and accurate books, records and accounts. The test should be based on reasonableness, not materiality or a minimum dollar threshold. Maintaining accurate books and records is not limited to the function of a finance department or limited to financial and accounting documentation or processes. Virtually all forms of documentation created by the business fall in scope and so all employees play a role in ensuring compliance with this requirement.

The control environment, the accounting system and control procedures are therefore all key components.

(viii) Solicitations

An entity or its staff must not solicit the payment of a bribe and should report any instance or attempt by any client or potential client to solicit such a payment. Firms will rely on these matters being escalated to management, including via the whistleblowing process. Via the various registers mentioned above, it may be possible to identify payments or transfers in value which are unusual. A solicitation may be at the heart of this activity.

(ix) Offers of employment, internships

Transfer of value has been mentioned above. Aside from the monetary value associated with an offer of employment, such offers including for example internships, may be considered to be offered by firms as bribes in order to secure a client relationship or favourable business terms. As part of the onboarding processes for staff, Human Resources (HR) departments have established procedures for offers of employment, including to interns and such procedures should incorporate appropriate due diligence checks, for example screening against sanctions lists, identification of public officials, PEPs etc. These checks should enable a firm to identify whether the recruitment process was conducted in a fair and transparent manner as well as allowing them to raise any issues relating to staff prior to employment. Cases could arise where a 'connected' candidate is selected for a particular role rather than the best candidate. Additionally, if any offer is made at the request of, or connected to a public official with whom a firm is dealing with in order to obtain or retain business, there must be appropriate pre-approval. HR or the business should raise issues initially with pre-approval raised to the relevant compliance department. The effectiveness of and adherence to the pre-approval process should be regularly checked.

(x) Dealings with third parties, agents and intermediaries

The programme needs to consider risks associated with third parties who are paid a fee to act on the company's behalf. Examples of third parties include agents and other intermediaries, consultants, representatives, distributors, contractors and suppliers, consortia, and joint venture partners. Processes around the engagement and ongoing monitoring of third parties should be well established, with appropriate senior management oversight for higher risk engagements. A company may find it beneficial to risk rate all of its third party dealings, in order to adopt a proportionate and risk based approach. Internal processes should at least include: (a) properly documented risk based due diligence before engaging higher risk third parties; (b) informing such third parties of the organisation's commitment to complying with anti bribery laws; (c) ensuring third parties sign a legal contract which contains appropriate anti bribery and corruption clauses and termination rights; and (d) monitoring periodically, on a risk based approach, those third parties who pose higher risk receiving more frequent and in depth checking and monitoring.

E. MIS/Reporting

An effective ABC Programme will include regular reports to senior management. Senior management needs to know how well an ABC Programme is protecting the firm from breaching laws or regulation or subjecting the firm to unacceptable levels of financial or reputational risks. Each firm will configure such reports to illustrate how well controls are operating to mitigate the risks that have been identified. The monitoring and controls mentioned above should be included within such reporting. If any trends or gaps are identified, these should be used to direct the compliance programme.

Across the industry, reporting relating to ABC within firms is not as well established as say, for AML or sanctions, and different firms will be at different levels of experience in managing ABC risks. A firm may experience challenges in obtaining data from areas such as finance or HR where those areas have not previously been required to monitor their operations for bribery or corruption, seeking to adapt existing systems for purposes for which they may never have been originally intended. Continued open dialogue with these areas and compliance support will be required to ensure that any required system or procedural changes are implemented. Having the 'tone from the top' is essential here to release budgets required to make such enhancements.

F. Record keeping

Accurate Books and Records & Internal Controls are an essential part of an ABC Programme. Slush funds,

misclassification of expenses, false invoices, dual general ledger accounts and misuse of petty cash are all ways employees can arrange bribe payments. Effective internal controls and accurate record keeping is an essential component of a compliance programme to detect and prevent bribery.

2. Designated Compliance Officer

Especially in the larger firms, in order to manage an effective ABC Programme there should be a specific individual with overall responsibility. The designated officer should have the appropriate level of expertise, authority and support in order to successfully run the programme and will be responsible for designing strategy, identifying, managing and reporting risks and having suitable controls to manage risks which are regularly tested. They will make available clear policies and guidelines and ensure appropriate escalation processes are in place.

3. Training Programme

In some cases, it may also be appropriate to extend the training to external parties such as suppliers or third party agents who are deemed particularly high risk.

4. Independent Testing

As well as relevant departments undertaking testing of the effectiveness of their monitoring and control tasks, this should also be tested independently. A compliance department may rely on a local assertion that controls are operating effectively but should verify this assertion by completing its own testing. For example, an HR department may state that its controls for identifying Public Officials when onboarding new staff and for existing staff are operating effectively. Or a finance department may assert that controls to identify unusual payments to third parties are working effectively. Compliance should verify these assertions independently. Internal audit functions will also undertake testing of the effectiveness of controls and will take into account local testing as well as compliance testing that has taken place.

The frequency of testing should be risk-based, can vary and can also be dependent on whether there is a known control weakness. The results of all testing should be raised to the appropriate fora for review.

Anti-Fraud Programme

A proficient anti-fraud programme ensures the risks from fraud to an organisation are minimised to the extent that the business can operate without unnecessary constraints. A culture with a zero tolerance approach to fraud when combined with a strong code of business ethics is engendered by senior management. Unlike AML, Sanctions and Bribery and Corruption, losses incurred due to fraud are immediately felt on profit and loss accounts. It is much easier to quantify and forecast fraud loss than for the other areas. A firm's approach to fraud risk management should be risk based and targeted, with the following elements tailored towards fraud detection and prevention:

Anti-Fraud Programme - Core Elements	
1	Policies, procedures and controls
2	Designated compliance officer
3	Training programme for employees
4	Independent audit function to test the programme

Source: Author

An Anti-Fraud Programme should operate around a set of high level principles, including:

- a) documenting and distributing a fraud control strategy that is an inherent part of the organisation's governance structure; this should include the expectations upon board directors, senior management and all employees to manage fraud risks.
- b) implementing a written fraud policy which outlines the actions for employees to take when fraud is suspected and that outlines the organisation's approach to fraud investigation to ensure consistency of approach.
- c) fraud risk assessment framework as part of an annual monitoring programme. This should identify the potential fraud risks arising from the products and services of the organisation.
- d) establishing and applying prevention techniques to avoid potential key fraud risk events and mitigate possible impact on the organisation.
- e) establishing detection techniques to uncover fraud events when preventive measures fail or unmitigated risks are realized.
- f) implementing a reporting or whistleblowing process to encourage employees to report suspicions of potential fraud.

1. Policies, Procedures & Controls

A. Code of Conduct/Specific Policies

Firms must convey a clear stance against fraud, usually in its code of conduct that it will not tolerate staff fraud or client fraud. As part of a firm's fraud risk management strategy, there should be a written policy, available to all employees which explains the expectations of the firm's board of directors and senior management to the issue of fraud.

Additionally as part of the fraud risk governance, a firm should include written policies and procedures to manage fraud risks. These procedures may include (but not limited to):

- a) whistleblowing and suspicion reporting for internal incident management
- b) information barrier policies
- c) bribery & corruption position statements
- d) segregation of internal controls and processes
- e) fraud awareness training
- f) fraud risk assessments
- g) continuous monitoring or surveillance
- h) systems access protocols

Firms will usually have a regular fraud risk management committee that meets to discuss the direction and effectiveness of its Anti-Fraud Programme.

Firms should also consider the ways in which it can reduce the incentives to committing or becoming involved in fraudulent activity. There should be increased emphasis on disincentives being built into performance management and remuneration policies. The threat of disciplinary or legal action can also act as a disincentive. However, as there will always be a risk of fraudulent activity occurring, a firm will place greater reliance on the strengths of its systems and controls in place to prevent and detect fraudulent activity.

B. Detection and SAR Filing

All instances and attempts of fraud should be investigated thoroughly and in a timely manner. Such activity should be considered for external reporting, whether to regulators, law enforcement or financial intelligence units.

A firm must put in place an investigation process to ensure that when fraud is suspected and reported it will be investigated in accordance with relevant rules of evidence, chains of custody and subsequently considered for reporting requirements (board, legal, regulatory or disciplinary). The investigation protocols should ensure that appropriate teams are alerted and

involved if necessary. Dependent upon the severity of the allegation, the investigating officer may need to involve HR, legal or compliance unit and/or the management committee or board. The protocols will, to some extent, be dictated by the local approach and lines of responsibility, for example, a specific anti-fraud function or embedded within a local risk unit or within the legal or compliance function. Ideally, investigations should be graded according to financial or other relevant thresholds or anticipated regulatory or reputational outcomes. This may depend on the volume and type of fraud exposure within an organisation and will assist in conveying the severity of the investigation to senior management.

Behavioural Red Flags

Most occupational fraudsters' crimes are motivated at least in part by some kind of financial or other pressure. In addition, while committing a fraud, an individual may frequently display certain behavioural traits associated with stress or the fear of being caught. These behavioural red flags can often be a warning sign that fraud is occurring. According to the Association of Certified Fraud Examiners 2012, Report to the Nations, a list of 16 common red flags were identified. The four most frequently cited in order were the following: The fraudster living beyond his or her means (36%), experiencing financial difficulties (27%), having an unusually close association with vendors or customers (19%), and displaying excessive control issues (18%). Then followed in order the following: Divorce/ Family problems, wheeler dealer attitude/ Irritability, Suspiciousness or Defensiveness, Addiction problems, Past employment related problems, Complained about inadequate pay, Refusal to take vacations, Excessive pressure from within organisations, past legal problems, Complained about lack of Authority, Excessive family/peer pressure for success and Instability in Life Circumstances.

C. Risk Assessment

As with AML risk assessments inherent risk ratings and net or residual risk ratings are often used to measure known risks. For fraud, the first step is identifying fraud risk that a firm is exposed to and then assessing the extent of that exposure, focussing of course on the major fraud notes as fraud can literally exist almost anywhere.

Across firms, the following areas should be considered as presenting increased fraud risks:

- i) Segregation of duties
- ii) Internal fraud: employee theft, fraud and unauthorised trading
- iii) External fraud or theft

- iv) IT governance
- v) Procurement
- vi) HR
- vii) Finance: inappropriately reporting and concealing assets or information
- viii) Whistleblowing

D. Monitoring and controls

Suitable monitoring and controls need to be in place both to prevent and detect instances of fraud. Controls will never eliminate the risk of fraud completely. Therefore, a firm should implement flexible techniques to deal with the frauds that have occurred. Weak controls in this area will increase opportunities for fraud to occur. In order to undertake any fraud, there must be an element of corruption and the controls required to prevent and detect corruption will overlap with fraud controls to a large extent. Below are some examples of the controls one would expect within an Anti-Fraud Programme:

(i) Segregation of duties

One of the ways in which frauds can occur within a firm is where individuals who are able to enter payment data also have approval rights for that payment. So in preventing fraud, adequate procedures and system access restrictions need to be in place which guard against the likelihood that someone committing fraud would be able to cover their tracks. Approval of invoices, payments etc. should be independently conducted to provide comfort that they are being made in the correct and legal manner. There are many further areas where segregation is appropriate and risk should be accordingly assessed.

(ii) Internal fraud

There are a number of ways in which employee theft, fraud and unauthorised trading can be prevented. It relies upon the necessary controls being in place, being undertaken systematically and their effectiveness being regularly tested. Examples include system restrictions which do not allow certain staff to divert client funds into personal accounts, profit and loss reports for desks to monitor for any trading anomalies, or approval controls in place for travel expenses, amongst others. Firms should also consider monitoring staff who do not observe block leave or appear to be working excessive hours.

(iii) External fraud or theft

Preventing external fraud is a huge challenge due to the dynamic nature of the threat. In one aspect understanding the nature of the threat clearly helps to focus preventative and detective control efforts. Typically a fraudster is targeting either access to

confidential data or seeking ways of getting funds paid away from an account. In the case of the latter, what typically proceeds a fraudulent payment attempt is an attempt to access client data and potentially even change certain elements of static data (phone records or address details) in order to re-route potential callbacks and divert mail away from a genuine client, thereby potentially widening the window in which fraud can be committed undetected. Key to preventing such events is strong, dynamic authentication controls both at the payment of payment execution requests and changes to client static data. Knowing your client is the key weapon in detecting unusual account changes or transactional requests. However, as technology is enabling a myriad of new ways to make payments, the nature of the fraud modus operandi evolves too. Fighting fraud is never a static business, it's more akin to an arms race with both sides constantly "tooling up" to outsmart the other!

Theft usually represents itself in a more physical way, such as a cash counter or ATM robbery. However, here the gains are limited, so again the nature of the threat has evolved into stealing client data, access codes and intellectual property electronically. Combating cyber threats requires a sophisticated approach to controlling data and securing it in a resilient IT environment.

(iv) IT governance

All IT landscapes will have known vulnerability points. Assessing these and actively managing them to resolution is key to ensuring the opportunity for a fraudster to exploit a weakness is minimised. A common feature of rogue trading events within investment banking is the exploitation of systems when back office personnel move to a front office role. Their ability to circumvent system protocols, often enabled through not having old access rights to back office systems rescinded can be a key enabler of not only the fraud being committed, but also going undetected for lengthy period of time. As per all fraud threats, IT threats are dynamic and evolving in line with technology and business strategy. Investment banks' activity in high frequency trading is another great example of a new scenario in which fraud or a malicious act can be committed en masse. In this instance, proper IT governance needs to ensure that malicious or manipulative coding or algorithms cannot be entered into a system, with a fail-safe (kill switch) facility enabled "just in case" anything slips through in order that future "flash crash" disasters can be avoided. IT governance basics, such as logical access controls to systems, controlling of peoples access rights and then monitoring for potentially toxic access combinations are all great ways to prevent unwanted events.

(v) Procurement

Contracts should be awarded fairly, relationships with suppliers should be managed with clarity and transparency and payments for goods or services should be made in accordance with contract terms. Along this journey, there are many opportunities for fraud to occur. There needs to be a clear process when selecting vendors and there should be appropriate approval (for example, authorised signatories) in place, particularly for the larger contracts, to ensure the risk of impropriety is minimised. Staff managing these relationships should be made aware of the possibility that they may be asked to take bribes to secure selection or negotiate favourable terms. Standard term contracts should be used, with any variations being approved by management.

Committees are likely to be in place that require a robust justification for selection of a supplier. Throughout the relationship, suppliers may submit false invoices or staff may create false invoices from suppliers in order to obtain and divert ill-gotten gains. Finance departments will often be required and best placed to undertake analysis of invoices received and amounts paid to ensure they reconcile. Relationships need to be monitored on a periodic basis, and this should take place independently. A review which is not independent increases the risk that those perpetrating a fraud may be able to conceal their objective, method and gains/losses.

There is also a natural link here to bribery and corruption: suppliers may try to bestow lavish gifts or entertainment to those staff at a firm who are considered to be influential in securing favourable contract terms and/or are signing engagement contracts. Hence, transparent processes in procurement and in recording and independent analysis of gifts and entertainment (given and received) ensures bribery and corruption risks are minimised.

The provision of company credit cards should require an approval process to ensure visibility of who is given a card. Company credit card spending should also be closely reviewed to ensure appropriate items are being procured or purchased from appropriate sources and that they are in line with what one might ordinarily expect for that individual's role at a firm. Most firms will require credit card expenditure to be reconciled monthly by card holders.

(vi) Human Resources

Whilst fraud risks exist with HR, such as payroll fraud, these tend to be comparatively modest ticket value frauds. Where HR's role is more crucial is ensuring

they execute their duty as a gatekeeper and supervisor in the fight against insider fraud. The insider threat is highly varied – fraud occurs at every level from junior administrative staff to directors and chief executives. Top performers and long-serving senior directors are liable to slip through the net, at least until they make a major mistake. Finance departments are unlikely to question the expenses of a director who has been with the company for a long period and delivered good results – or the behavior of a trader who delivers numbers greatly in excess of the market norm. Often, fraudulent employees may appear to be the most diligent in the department.

Ideally, these individuals need to be excluded from the company before they wreak untold damage, in monetary and reputational terms, by a recruitment process that is as alert to fraud risk as it is to job competence. This puts HR into the front line. They create the initial application form, vet it for inconsistencies, downright lies and unexplained gaps and then interview the candidate.

(vii) Finance

Financial statement fraud schemes tend to be classified as ones in which an employee intentionally causes a misstatement or omission of material information in the organisation's financial reports (e.g., recording fictitious revenues, understating reported expenses or artificially inflating reported assets). The role of the finance team in preventing and detecting such events focusses heavily on reconciliation and verification protocols. For example, balance sheet verification, books and records reconciliations (including suspense and non-personal accounts) and validating manual adjustments and changes to static data records are all key areas which have typically been exploited. Alternatively, one could summarise the key control in one word; skepticism. Skepticism involves the validation of information through probing questions, the critical assessment of evidence, and attention to inconsistencies. Skepticism increases not only the likelihood that fraud will be detected, but also the perception that fraud will be detected, which reduces the risk that fraud will be attempted.

In 2002, WorldCom, under Bernie Ebbets one the world's largest telecommunications companies (at its peak worth US\$160bio) filed for bankruptcy following an US\$11bio accounting fraud. WorldCom made major accounting misstatements that hid the increasingly perilous financial condition of the company. As enormous as the fraud was, it was accomplished in a relatively mundane way, with more than US\$11bio in false or unsupported accounting entries were made

in WorldCom's financial systems in order to achieve desired reported financial results. Whilst WorldCom was the largest accounting scandal at the time, it had many predecessors and would be succeeded soon after by the like of Enron led by Ken Lay. For more details see Part 1, Section 1, Fraud and Part 2, Section 7, Criminals & Terrorists.

(viii) Whistleblowing

Whistleblowing is still the singular most effective means of detecting unwanted behavior. A well communicated policy, supported by proper training and awareness amongst employees is key to achieving good results. The Policy should protect staff from any adverse consequences or retribution where a disclosure is made in good faith, even if it turns out that there was no substance to the concern. The presence or absence of a reporting hotline has an interesting impact on how frauds are discovered. According to the ACFE's 2012 Report to the Nations, organisations with some form of hotline in place saw a much higher likelihood that a fraud would be detected by a tip (51%) than organisations without such a hotline (35%). An interesting trend is the financial rewarding of whistleblowers, introduced in the US in 2011 through the Dodd Frank Act. This offers monetary awards to eligible individuals who voluntarily provide original information that leads to successful commission enforcement actions resulting in the imposition of monetary sanctions over US\$1,000,000, and certain related successful actions. Awards are required to be made in the amount of 10% to 30% of the monetary sanctions collected, with the largest award made to date totaling US\$14mio. Since the introduction of this act, the volume of reported whistleblowing cases continues to climb, with 3,001 whistleblower reports received in 2012. The most common complaint categories reported by whistleblowers were Corporate Disclosures and Financials (18.2%), Offering Fraud (15.5%), and Manipulation (15.2%).

E. MIS/Reporting

The provision of management information is essential to any anti-fraud programme. Incidents of fraud should be reported. As fraud loss is quantifiable, it is easier than with AML, bribery or corruption or sanctions to identify pattern changes which could indicate fraud has taken place. Such reports must be reviewed carefully and escalated to senior management, including the Board where necessary. Profit and loss, supplier payment and travel expense are all examples of reports that could be used to identify fraudulent activity. The simple question of whether something is 'too good to be true' can be ignored at a firm's peril. Such challenge should be ingrained in all staff charged with analysing fraud

metrics. Senior management should also be made aware of legal and regulatory developments in the area as this may affect a firm's risk appetite for certain products or services that start to carry a higher fraud risk. Firms will always need to take a risk based approach to fraud mitigation and a firm's risk appetite for fraud loss can be defined in monetary terms. It is also easier with fraud to calculate and predict savings made as a result of the anti-fraud programme. For example, if a fraud loss had occurred due to an exploited IT deficiency which is then mitigated, the saving is at least that initial fraud loss. Firms may incorporate fraud case management systems to generate fraud related data but this is certainly more complex to implement and keep accurate in larger firms. Reporting of fraud trends and incidents will also help other parts of a firm ensure that they have systems and controls in place to prevent future occurrences. As part of this strengthening of an Anti-Fraud Programme, firms should also make use of the plethora of industry guidance and updates on fraud trends available.

F. Record Keeping

Not only will accurate record keeping assist a firm in the event of any legal or regulatory investigation but it will also help a firm undertake its own investigation into fraudulent activity. Whether it is keeping a record of how a beauty parade of suppliers led to a recommendation to pick a certain supplier or it is a keeping a record of incidents of fraud so as to undertake trend analysis, records need to be kept accurately and be retrievable. Inventories of fraud incidents must be kept in order to assist reporting and as a way of learning from past control weaknesses. Throughout a client relationship or the general operation of a firm, without appropriate record keeping, a firm will be less equipped to spot and manage fraud risks and fraudulent activity.

2. Designated Officer

A designated officer may be appointed to take charge of a firm's Anti-Fraud Programme, usually run from an operational risk environment, but with close collaboration with compliance where required. Such an officer will set the fraud strategy, have it endorsed by senior management/the board, organise a team to undertake specific parts of the programme and will also be expected to have visibility of all incidents of fraud or attempted fraud and fraud trends, as well as face off to external stakeholders, such as regulators and law enforcement.

3. Training Programme

Firms may either include fraud as a topic within general financial crime training or have a specific training module on fraud or a number of modules. In any case they must take a risk based approach to training and

maintaining awareness. When joining a firm, staff are usually a required to sign a firm's Code of Conduct, in which a firm will set out that it does not tolerate any fraud by any member of staff and the consequences for staff involved in fraudulent activity, both at and outside the firm. In any training on fraud, staff should be made of aware of a firm's stance on fraud, how to spot it, how to report it and the consequences of not conforming to the firm's policy on fraud. Departments or staff at a higher risk of fraud, e.g. payments, procurement, etc. should be identified and receive additional training which seeks to use case studies to illustrate the ways in which their roles could be susceptible to fraudulent activity and the red flags they should look out for when trying to identify fraudulent activity. Indeed, the learning points from any incidents or attempts of fraud should be used to direct the future of an anti-fraud programme. Fraud awareness programmes can also be used to good effect, especially in the higher risk departments, e.g. newsletters, poster campaigns, stationary with anti-fraud messages and reminders, etc.

4. Independent Testing

Within a firm there should be differing roles and responsibilities, for example:

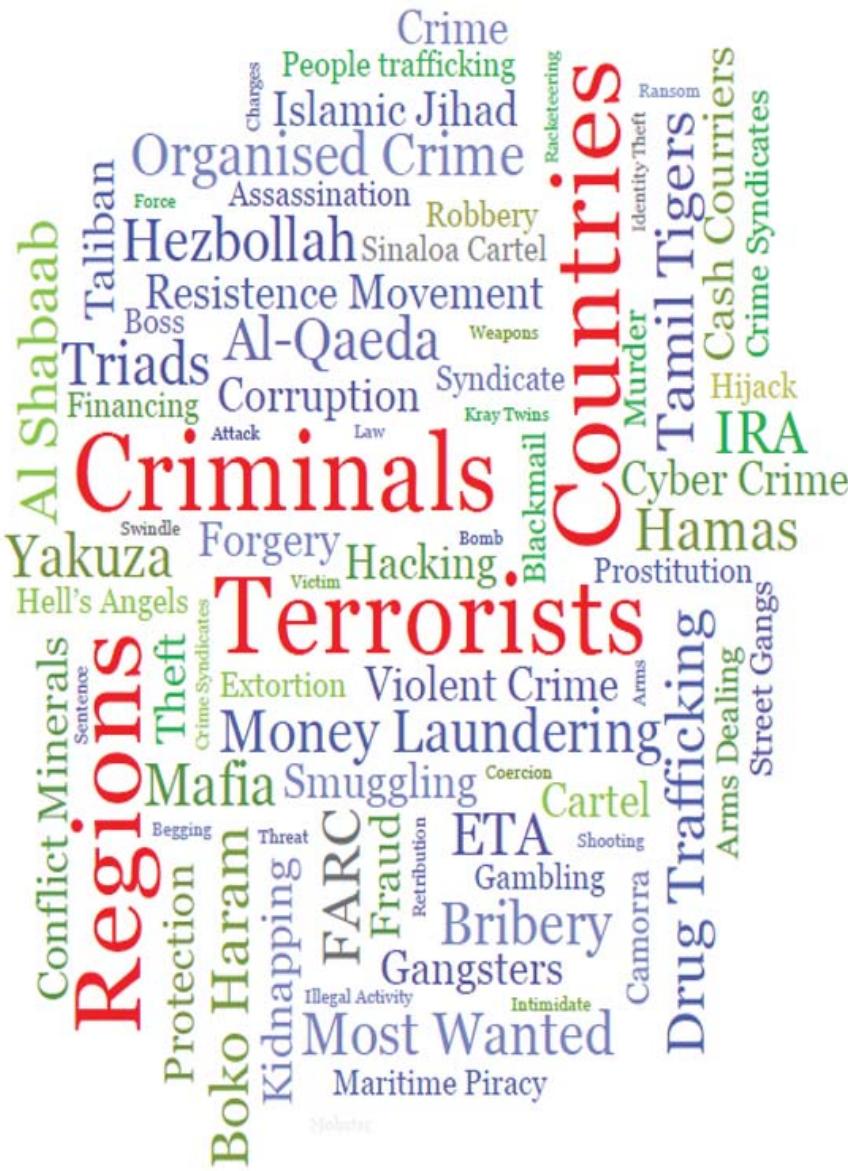
- a) oversight of fraud controls and risks
- b) design and implementation of fraud strategy
- c) independent audit and investigation functions
- d) monitoring and surveillance of internal processes and controls

A firm may designate such responsibilities to the board of directors, or the internal audit committee, a risk management function or at the micro level to all staff as part of their overall vigilance to identify and prevent fraud and manage fraud risk within their specific roles. It could be operational risk areas or compliance at a firm that undertakes fraud testing. As well as self-assessment, the Anti-Fraud Programme should be tested independently. Some firms will have a separate risk assessment and review department that will do this, whilst others will rely solely on internal audit to validate the effectiveness of the programme. Following a fraud incident, firms may well be expected to appoint external auditors to review its Anti-Fraud Programme. This may provide comfort to a regulator that fraud standards are improved but should not be relied upon as a one-off exercise. Continued learning is required from any review to ensure standards are maintained. The principles of good fraud management should be continually reviewed to ensure they remain appropriate for a firm.

Contents - Part 2

Section 5 - Regions, Countries, Criminals & Terrorists, 318	Introduction, 318	- Others, 610
Introduction, 319	Insider Traders, 611	
Africa, 321	Kidnappers / Robbers / Extortioners / Forgers, 625	
- North Africa, 322	Market Abusers, 629	
- West Africa, 326	Traffickers, 642	
- The Horn of Africa, 330	- Illicit Arms Traffickers, 642	
- Eastern Africa, 332	- Drug Traffickers (Organised Crime), 649	
- Central Africa, 337	- Goods Traffickers, 655	
- Southern Africa, 341	- Human Traffickers, 656	
Middle East, 347	Terrorism Financiers, 658	
Asia, 370	WMD Proliferation Financiers/Sanctions, 664	
- Southern Asia, 370		
- South East Asia, 397	Section 8 - Enforcement Cases, 670	
- Eastern Asia, 404	Introduction, 671	
- Central Asia, 414	- Chronology of FI Major Enforcement Cases over the last 25 years, 673	
Oceania, 417	- Enforcement Cases, 675	
Americas, 419		
- US, Canada and Mexico, 420-	Outlook Cases/2014 and beyond, 738	
- Caribbean, 443	Breaking News, 739	
- Central America, 446	Notes, 745	
- South America, 451	Abbreviations, 813	
Europe, 469	Index, 814	
- Eastern Europe, 470	Reviews of this Book, 845	
- Western Europe, 485		
Section 6 - Terrorist Attacks, 508		
Introduction, 509		
Chronology of the Worlds Worst Terrorist Attacks over the last 100 years, 511		
Chronology of the Worlds Worst Airline Attacks by Terrorists, 531		
Section 7 - Criminals/Cases, 540		
Introduction, 542		
Corruption		
- Individuals/PEPs, 543		
- Corporates, 561		
Environmental Crime, 568		
Fraudsters, 569		
- Accounting Fraudsters, 569		
- Advanced Fee Fraudsters, 581		
- Hedge Fund / Investment Co Fraudsters, 582		
- Ponzi - Pyramid Schemes, 586		
- Rogue Traders, 588		
- Private Banker Fraudsters, 606		
- Tax Fraudsters - Tax Evaders, 607		

Section 5 - Regions, Countries, Criminals & Terrorists



- Introduction, 319
Africa, 321
- North Africa, 322
- Special Focus 1 - Al-Qaeda in the Islamic Maghreb, 325
- West Africa, 326
- Special Focus 2 - Boko Haram, 328
- The Horn of Africa, 330
- Special Focus 3 - Al Shabaab, 331
- Eastern Africa, 332
- Central Africa, 337
- Southern Africa, 341
Middle East, 347
- Special Focus 4 - Hamas, 354
- Special Focus 5 - Hezbollah, 357
- Special Focus 6 - Al-Qaeda in Iraq, 359
- Special Focus 7 - Al-Qaeda in the Arabian Peninsula, 365
Asia, 370
Southern Asia, 372
- Special Focus 8 - Al-Qaeda, 372
- Special Focus 9 - Taliban, 377
- Special Focus 10 - Liberation Tigers of Tamil Eelam, 395
South East Asia, 397
Eastern Asia, 404
- Special Focus 11 - Triads, 407
- Special Focus 12 - Yakuza, 411
Central Asia, 414
Oceania, 417
- Australia / New Zealand, 417
- Pacific Islands, 418
Americas, 419
United States, 420
- Special Focus 13 - American Mafia, 427
- Special Focus 14 - Outlaw Motorcycle Gangs, 429
Canada, 432
Mexico, 435
- Special Focus 15 - Mexican Drug Trafficking Organisations, 437
Caribbean, 443
Central America, 446
South America, 451
- Special Focus 16 - FARC / Revolutionary Armed Forces of Colombia, 460
- Special Focus 17 - Colombian Drug Cartels, 462
Europe, 469
Eastern Europe, 470
- Special Focus 18 - Russian Mafia, 479
Western Europe, 485
- Special Focus 19 - ETA / Euskadi Ta Askatasuna, 488
- Special Focus 20 - Italian Mafia, 494
- Special Focus 21 - Provisional Irish Republican Army, 500

Introduction

Across the world, in all habitable continents, money laundering risks present themselves, through in particular, organised criminal gangs or terrorist groups and whilst each may have distinctive hallmarks, they often share similar motives and characteristics too. Organised Criminal gangs can be found in most countries in the world with the most successful exploiting key points of interest along the value chain of the most profitable criminal industries whether drugs, people or products in origin transit and destination countries. Concentrations do appear in many of the Worlds largest and most successful Countries and Cities, where trade, demand and opportunities abound, but many like Terrorist Groups can also be found in most regions of the world though increasingly they tend to flourish where they can find either a safe haven or where there is sufficient instability or where strong government control is missing.

Criminals and terrorist have something unique in common, they refuse to play by the rules societies have laid down, they prosper and exploit weak and unstable situations and they manipulate situations for their personal goals. Where both seek to concentrate power and authority, to control their direct and surrounding environments, ostensibly in the case of organised crime for financial reward and in the case of terrorists for political ideals, leading to political revolution, each will fail unless they reform, each have a fundamental deficit and lack any true legitimisation. As they grow, they will bribe for protection, apply violence to achieve their aims, generate funds from propaganda and/or from profitable criminal activities, propagate their ideologies and care less about the consequences of their actions. As they create their mayhem, they rely on the rest of us to be intimidated, to feel helpless and overawed.

History shows that whilst new threats emerge, quietly at first, they begin to be understood and eventually are despatched. A gangland murder or a terrorist attack creates both media attention, but also equally, perhaps as a result requires a political response. The greater the crime the greater the response. The shorter the conflict the greater the intensity. The longer the conflict, the wiser the belligerents.

Whether the threat from terrorists versus that posed by organised crime is greater is arguable, certainly the terrorist impact from attacks is undeniable, and certainly the misery created to many from organised crime is real.

Whilst it was considered that there was a distinct separation between the two, these distinctions can become blurred and it should be assumed that both learn from each other, and both need to be aggressively resisted. After bin Laden was killed in 2011 in Pakistan, the head of an organised criminal gang became the most wanted man in the world, at least according to US authorities. Joaquin Guzman Loera (El Chapo)¹ is the leader of the

Mexican Sinaloa Cartel, that controls a significant part of the drug trade into the USA also earning the title as "the world's most powerful drug trafficker." Whilst the Sinaloa Cartel jealously and violently defends its interests it both competes and works with other organised gangs both in Mexico and around the world. The existence of organised criminal gangs on every continent in virtually every country remains a significant threat to society, as does the existence of terrorist groups.

There are no government published lists covering the Worlds organised criminal gangs, nor do governments publish and/or rank organised criminal gangs where membership size, success in generating proceeds, harms caused etc are collected and made available, though there are private publications relating to one or more gangs and a number of authors that have tried to collect information on some of the most important. For terrorist groups, they exploit weaknesses in society and in governments, promoting extreme ideology and combining this with the capacity and willingness to employ violence as a principal tactical tool. Whilst there are numerous lists issued by countries, the names of groups are varied with only a few that consistently include the same groups, with a global consensus surrounding Al-Qaeda and Al-Qaeda affiliates but not too many more. For more information about Organised Crime and Terrorists, in particular, Terrorist Financiers see Part 1, Section 1. For more details about many of the worst terrorist attacks see Part 2, Section 6.

In this Part 2 Section 5, the material is split into Regions, and then sub Regions with particular focus on Countries of particular interest from a money laundering, organised crime and terrorism perspective, and includes the most powerful criminal gangs and the most dangerous terrorist groups operating still today and some of histories most notorious, are briefly profiled, with 20 of the most significant profiled in more detail. These criminal gangs and terrorist groups are also placed into the country and regions from where they have their origins or most significant operations.

As far as Regions and Countries are concerned there is an increased focus on Africa; the Middle East; Latin America; Eastern Europe and Asia, whilst at the same time also including Western Europe and North America also. More detailed country profiles include the BRIC countries, the CIVETS and the so called Next 11, namely, Brazil, Russia, India and China (BRIC) and Colombia, Indonesia, Vietnam, Egypt, Turkey and South Africa (CIVETS) and Bangladesh, Egypt, Indonesia, Iran, Mexico, Nigeria, Pakistan, Philippines, Turkey, South Korea, and (as with the CIVETS list) Vietnam (Next 11). Country Focus is also increased for Countries that are home or materially affected by Organised crime groups or terrorist organisations and are subject to sanctions and embargoes as well as countries identified by FATF as having Strategic AML deficiencies or where counter measures are required.

In this Part 2, Section 5 Regions, Countries, Criminals and Terrorists, the sources are all publicly available and in particular the following key sources have been used.

- Wikipedia - www.Wikipedia.com; Country Profiles and money laundering and financial crime information from the The US Central Intelligence Agency (CIA) World Factbook 2013-14. <https://www.cia.gov/library/publications/the-world-factbook/index.html> and from the 2013 International Narcotics Control Strategy Report (INCSR), which is an annual report by the Department of State to Congress prepared in accordance with the Foreign Assistance Act. It describes the efforts of countries to attack all aspects of the international drug trade, money laundering and financial crimes.

- Wikipedia - http://en.m.wikipedia.org/wiki/List_of_designated_terrorist_organisations; which is a list of designated terrorist organisations by the UN, EU, and by certain national governments, including the US Canada, Australia, UK, France, India Turkey. National resources are also utilised including for example the US Department of the Treasury's, Office of Foreign Assets Control (OFAC) for details see: <http://www.treasury.gov/about/organisational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>. Many organisations that are accused of being a terrorist organisation deny using the terrorism label;

- from the National Consortium for the Study of Terrorism and Responses to Terrorism, better known as START, a university-based research center, based at the University of Maryland, and a Center of Excellence of the U.S. Department of Homeland Security, focussing on terrorism in the US and around the world. START's materials include profiles for many of the most important past and present terrorist groups and details of over 100,000 terrorist incidents. START can be found at <http://www.start.umd.edu>.

- from the South Asia Terrorism Portal, (SATP), which is the largest resource of publicly available information on terrorism, low intensity warfare and ethnic/communal/sectarian strife in South Asia, in particular on the Indian sub continent region, covering the profiling of terrorist and extremist groups and incidents. The SATP is run by The Institute for Conflict Management, an Indian non-Profit Society set up in 1997 in New Delhi. The SATP can be found at: <http://www.satp.org>.

- from the Terrorism Research & Analysis Consortium (TRAC), which gathers comprehensive terrorist information about groups and incidents in cooperation with a team of 2800 experts. TRAC can be found at <http://www.trackingterrorism.org/about>

- and from the International Centre for Political Violence and Terrorism Research (ICPVTR) which is a specialist centre within the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore, which conducts research on politically motivated violence and at mitigating its effects on the international system. The ICPVTR can be found at: <http://www.pvtv.org>

UN Designated Terrorist Organisations

The Al-Qaeda Sanctions Committee was established on 15 October 1999 by the Security Council with the adoption of resolution 1267 for the purpose of overseeing the implementation of sanctions measures imposed on Taliban-controlled Afghanistan for its support of bin Laden. The sanctions regime has been modified and strengthened by subsequent resolutions, so that the sanctions measures now apply to designated individuals and entities associated with Al-Qaeda wherever located. On 17 June 2011, the Security Council decided to split the Al-Qaeda and Taliban sanctions regime. Resolution 1989 (2011) stipulates that the sanctions list maintained by the Security Council Committee established pursuant to resolution 1267 (1999) will henceforth be known as the "Al-Qaeda Sanctions List" and include only names of those individuals, groups, undertakings and entities associated with Al-Qaeda. The applicable resolutions requires all States to: freeze the assets of, prevent the entry into or transit through their territories by, and prevent the direct or indirect supply, sale and transfer of arms and military equipment to any individual or entity associated with Al-Qaeda as designated by the Committee. The primary responsibility for the implementation of the sanctions measures rests with Member States and effective implementation is mandatory.

The following entities are on the Al-Qaeda Sanctions List:² Abu Sayyaf Group; Egyptian Islamic Jihad; Al-Qaeda; Al Rashid Trust; Armed Islamic Group; Asbat Al-Ansar; Harakat Ul-Mujahideen / HUM; Islamic Army of Aden; Islamic Movement Of Uzbekistan; Libyan Islamic Fighting Group; Makhtab al-Khidamat; The Organisation of Al-Qaeda in the Islamic Maghreb; Wafa Humanitarian Organisation; Jaish-i-Mohammed; Jam'ah Tâ'awun Al-Islamia; Rabita Trust; Ummah Tameer E-Nau (UTN); Afghan Support Committee (ASC); Revival of Islamic Heritage Society; Al-Haramain Islamic Foundation (various branches and offices); Eastern Turkistan Islamic Movement; Moroccan Islamic Combatant Group; Tunisian Combatant Group; Global Relief Foundation (GRF); Jemah Islamiyah; Benevolence International Foundation; Lashkar i Jhangvi (LJ); Ansar al-Islam; Islamic International Brigade (IIB); Riyadus-Salikin Reconnaissance and Sabotage Battalion of Chechen Martyrs (RSRSBCM); Special Purpose Islamic Regiment (SPIR); Djamar Houmat Daawa Salafia (DHDS); Al-Haramain Foundation (Indonesia); Al Furqan; Taibah International-Bosnia Offices; Al-Qaeda in Iraq; Lashkar-E-Tayyiba; Islamic Jihad Group; Al-Akhtar Trust International; Sanabel Relief Agency Limited; International Islamic Relief Organisation, (Philippines and Indonesia, Branch Offices); Rajah Solaiman Movement; Al-Qaeda in the Arabian Peninsula; Harakat-ul Jihad Islami; Emarat Kavkaz; Tehrik-e-Taliban Pakistan (TTP); Jemmad Anshorut Tauhid; Movement for Unity and Jihad in West Africa (MU-JAO); Ansar Eddine.

Africa



Africa is the world's second-largest and second-most populous continent, covering 6% of the Earth's total surface area and 20.4% of the total land area, home to approximately 1.0 billion people (as of 2009). Africa has 54 fully recognised sovereign states, 9 territories and three de

facto states with limited recognition. These States have borders which were largely drawn during the 19th Century when European Imperial powers engaged in a territorial scramble, occupying almost all of the continent apart from only 2 independent States, Ethiopia, known as "Abyssinia" and Liberia. Imperial rule largely continued until after the end of the Second World War, where colonial territories gradually obtained formal independence, for example, the first being Libya (1951); Tunisia and Morocco (1956); and Ghana (1957), with the rest following later.

Africa, particularly central Eastern Africa, is widely accepted as the origin of humans, with the earliest Homo sapiens (modern human) found in Ethiopia being dated to around 200,000 years ago.

Africa straddles the equator and encompasses numerous climate areas; it is the only continent to stretch from the northern temperate to southern temperate zones. It is thought that Africa most likely got its name, from the word "Afri" used to refer to the Carthaginians, descendants of the Phoenicia who lived in North Africa in modern-day Tunisia who were referred to as "Afri" meaning "dust" or "afar".

Under Roman rule, Carthage became the capital of Africa Province, which also included the coastal part of modern Libya. The Latin suffix "-ica" can sometimes be used to denote a land. The later Muslim kingdom of Ifriqiya, modern-day Tunisia, also preserved a form of the name. According to the ancient Romans, Africa lay to the west of Egypt, while "Asia" was used to refer to Anatolia and lands to the east. A definite line was drawn between the two continents by the geographer Ptolemy (85–165 AD), indicating Alexandria along the Prime Meridian and making the isthmus of Suez and the Red Sea the boundary between Asia and Africa.

An alternative possible source comes from the Berber peoples of North Africa where the word "ifri" meaning "cave" was a reference to this tribe as cave dwellers.

Africa can be divided up into numerous regions, from a simple divide of North Africa or the Maghreb made up largely of Arabs and considered part of the Arab World

and Sub Saharan Africa, or the rest of Africa, once called Black Africa, to the south. The Sahel is the transitional zone between the Sahara and the tropical savanna further South.

In North Africa there are only 6 Countries included, being Algeria, Morocco, Western Sahara, Tunisia, Libya and Mauritania. In Sub- Saharan Africa there are 49 countries, the largest of which by population are Nigeria, Ethiopia, Democratic Republic of Congo, South Africa, Tanzania and Kenya.

The World Bank works with 45 Countries, as many are considered less developed compared to other countries and regions of the world, with many of these countries having weak public institutions, high levels of corruption and poor records on human rights. Many who live in Sub Saharan Africa live under desperate conditions, with natural disasters and civil wars aggravating the situation, and with close to 10 million internally displaced with approximately the same ending up in other countries as refugees. The largest refugee camp in the world, is in Africa, in Dadaab in Kenya, close to the border with Somalia with over 500'000 inhabitants.

Valuable economic sectors include oil, mining or tourism, but these are only available to a few and many of the rest still rely on agriculture, which for many remains at the level of subsistence farming.

Under such circumstances a number of serious criminal activities have flourished. These include, Drug Trafficking, Smuggling, Human Trafficking and Terrorism. For example as far as Drug Trafficking is concerned, according to the UN Office on Drugs and Crime (UNODC) 27 % of Europe's cocaine enters through West Africa. Ghana, Sierra Leone, Mali and Nigeria are the most common entry points for Cocaine from Colombia. From there the drugs are transported up North through the Sahara.

Corruption remains a significant problem in Africa with 9 out of the 20 worst ranked countries by Transparency International in its 2012 Corruptions Perception Index with Angola, DR Congo, Libya, Equatorial Guinea, Zimbabwe, Burundi, Chad, Sudan and Somalia all included.

Not surprisingly, trafficking of human beings is considered as one of the fastest growing sectors of criminal activity in the region, exploiting the dire situation of many. Finally, terrorist activities and related weapons dealers are present in many countries.

Sub-Saharan Africa can also be divided into regions, with Countries falling into one or more of the following regional groupings, West Africa, the Horn of Africa, Eastern Africa, Central Africa and Southern Africa.

North Africa



Often described as the Maghreb which is defined as the region west of Egypt, being the region including the Atlas Mountains and the coastal plains of Morocco, Algeria, Tunisia, and Libya, and since the 1989 formation of the Arab Maghreb Union, by the inclusion of a fifth nation,

Mauritania, and of the disputed territory of Western Sahara (mostly controlled by Morocco). Maghrebis were once known as "Moors". Partially isolated from the rest of the continent by the Atlas Mountains and the Sahara desert, inhabitants of the northern parts of the Maghreb have long had commercial and cultural ties to the inhabitants of the Mediterranean countries of Southern Europe and Western Asia, going back at least to the Phoenicians in the 1st millennium BC (the Phoenician colony of Carthage having been founded, according to tradition, in what is now Tunisia circa 800 BC).

Algeria

After more than a century of rule by France, Algerian achieved its independence in 1962. Whilst the National Liberation Front (FLN), had largely dominated politics since independence, elections in 1991 led to success in the first round by the Islamic Salvation Front (FIS). The army began a crackdown on the FIS which escalated into an insurgency, which saw intense violence from 1992-98, resulted in over 100,000 deaths, many attributed to indiscriminate massacres of villagers by extremists. The Armed Islamic Group (GIA) emerged in 1992 as a splinter group of the FIS. The government however gained the upper hand by the late-1990s, and Abdelaziz Bouteflika won the presidency in 1999 in an election widely viewed as fraudulent and has retained the Presidency to this day. After the millennium, an amnesty offered to GIA members, with those continuing the struggle considered to have joined the Salafist Group for Preaching and Combat (GSPC) who in 2006 merged with Al-Qaeda to form Al-Qaeda in the Islamic Maghreb, which has launched an ongoing series of kidnappings and bombings targeting the Algerian Government and Western interests. The government in 2011 introduced some political reforms in response to the Arab Spring, including lifting the 19-year-old state of emergency restrictions.

Armed Islamic Group - Algeria

The Armed Islamic Group (GIA) emerged in 1992 as a splinter group of the Islamic Salvation Front (FIS), a body campaigning to establish an Islamic state in

Algeria. When this campaign appeared to be nearing success in Algeria, and an FIS electoral victory seemed imminent, the ruling military government cancelled forthcoming elections and installed exiled independence fighter Mohammed Boudiaf as the new president. This violation caused outrage and led to the establishment of the Armed Islamic Group. The US Department of State speculated that the GIA possessed "several hundred to several thousand" members. Other sources, including military personnel in Algeria, estimated that GIA operated with 1,300 -2,000 men supported by a network of 5,000-6,000 members. The organisation's funding was, for the most part, derived from criminal activity including extortion and bank raids. In terms of ideology the GIA adhered to the Salafist tradition; a distinct subdivision within the Islamic faith that believes in only the revelations of Mohammed and his companions. GIA considered itself to be engaged in a war against all infidels; a category GIA defined as encompassing non-Muslims and non-Salafist Muslims. Targets of GIA operations have included the Algerian government and its supporters, foreign governments believed to support the Algerian ruling party, and even singers of Rai music; an amalgamation of French, Spanish and Arabic musical traditions that has been deemed religiously offensive by GIA. Civilians have also become victims of GIA attacks, with journalists, intellectuals and those attending secular schools proving to be high risk social groups. Between 1993 and 1998 GIA claimed the lives of around 70,000 people, including more than 100 foreign nationals.

A characteristic form of violence perpetrated by GIA was to raid villages at night and slit the throats of their victims. GIA has also engaged in fighting with the FIS and rival armed Islamic group the Islamic Salvation Army (AIS). The AIS disputed GIA's claim to the just jihad in Algeria, asserting that its own campaign, which focussed primarily on combating government forces, was the rightful cause as it did not target civilians. GIA operations were also launched outside Algeria, focusing in particular on targets in France. For instance on 24 December 1994 GIA operatives hijacked an Air France plane scheduled to make a flight from Algiers to Paris. While the attempt was thwarted by French security forces who boarded the plane, the purported aim of the operation was to fly the aircraft into the Eiffel Tower. Another plot to execute a terrorist attack abroad was foiled in 1999 when GIA member Ahmed Ressam was apprehended attempting to cross the US-Canadian border in a car laden with explosives. The intended target of the attack was Los Angeles International Airport, where Ressam and his co-conspirators had planned to detonate the bombs on the eve of the millennium. After pardons were offered by the Algerian government to any GIA militants who surrendered and had not participated in civilian attacks, some sources have come to believe that the organisation has become inactive as a terrorist group. Members persisting in terrorist activities are thought to have been absorbed by the Salafist Group for Call and Combat (GSPC).

Western Sahara

Western Sahara is a disputed territory on the northwest coast of Africa bordered by Morocco, Mauritania, and Algeria. After Spain withdrew from its former colony of Spanish Sahara in 1976, Morocco annexed the northern two-thirds of Western Sahara and claimed the rest of the territory in 1979, following Mauritania's withdrawal. A guerrilla war with the Polisario Front contesting Morocco's sovereignty ended in a 1991 cease-fire and the establishment of a UN peacekeeping operation. As part of this effort, the UN sought to offer a choice to the peoples of the Western Sahara between independence (favored by the Polisario Front) or integration into Morocco. A proposed referendum never took place due to lack of agreement on voter eligibility. The 2,700 kms (1,700 miles) long defensive sand berm, built by the Moroccans from 1980 to 1987 and running the length of the territory, continues to separate the opposing forces with Morocco controlling the roughly 80% of the territory west of the berm. Ethnic tensions in Western Sahara occasionally erupt into violence requiring a Moroccan security force response.

Mauritania

Mauritania achieved its independence from France in 1960. Maouya Ould Sid'Ahmed Taya seized power in a coup in 1984 and ruled Mauritania autocratically for more than two decades. A bloodless coup in August 2005 deposed President Taya and ushered in military rule, which continues though Taya has been replaced and the current President Aziz. Mauritania has a largely informal and under-developed economy, a large informal trade sector, porous borders, and corruption in government and the private sector. Only an estimated 4% of Mauritanian adults have bank accounts, and informal banking and financial systems remain vulnerable to exploitation. In recent years, Mauritania has become a transshipment point for cocaine from South America intended for the European market. General smuggling, trafficking in vehicles stolen mostly in Europe, parallel financial networks, and the provision of logistical support for organised international drug traffickers are all serious problems. Because of increasing terrorist and illicit trafficking activities along the long and porous borders with Algeria and Mali, the Government of Mauritania has continued an aggressive campaign against corruption and the terrorist network of Al-Qaeda in the Islamic Maghreb.

Libya

The Italians supplanted the Ottoman Turks in the area around Tripoli in 1911 and did not relinquish their hold until 1943 when defeated in World War II. Libya then passed to UN administration and achieved inde-

pendence in 1951. Following a 1969 military coup, Col Muammar al-Gaddafi assumed leadership and began to espouse his political system at home, which was a combination of socialism and Islam. During the 1970s, Gaddafi used oil revenues to promote his ideology outside Libya, supporting subversive and terrorist activities that included the downing of two airliners, one over Scotland, another in Northern Africa, and a discotheque bombing in Berlin. UN sanctions in 1992 isolated Gaddafi politically and economically following the attacks. After 9/11 he agreed to end Libya's programme to develop weapons of mass destruction, and made significant strides in normalising relations with Western nations, including acceptance of responsibility for the terrorist bombings and to pay compensation. UN sanctions were lifted in 2003 as a result. Following the start of the Arab Spring, unrest erupted in Libya in early 2011. Gaddafi's brutal crackdown on protesters spawned a civil war that triggered UN authorisation of air and naval intervention by the international community. After months of fighting between government and opposition forces, including by the Libyan Islamic Movement for Change a successor Organisation to the Libyan Islamic Fighting Group, the Gaddafi regime was toppled in mid-2011 and replaced by a transitional government, which struggles to run the country today with regional militias still holding on to much power. As the new Government of Libya works to assert its elected authority, armed militias, former revolutionaries, tribes and clans within Libya engage in criminal activity for profit, including theft, weapons trafficking, and extortion. It is a transit and destination country for large numbers of migrants from sub-Saharan Africa and Egypt and is a destination and transit point for smuggled goods, particularly black market and counterfeit goods from sub-Saharan Africa. The markets remain primarily cash-based, and informal value transfer networks are present. Hawaldars are often used to facilitate trade and small project finance. Libya's geographic position, porous borders and limited law enforcement capacity make it an attractive transit point for narcotics. Corruption remains a serious problem. Libya is ranked 160 out of 176 countries in Transparency International's 2012 International Corruption Perception Index.

The Libyan Islamic Fighting Group (LIFG) - Libya
The Libyan Islamic Fighting Group (LIFG) was designated by the US as a Foreign Terrorist Organisation on December 17, 2004. In the early 1990s, LIFG emerged from a group of Libyans who had fought Soviet forces in Afghanistan and pledged to overthrow Libyan leader Muammar Gaddafi. In the years following, some members maintained an anti-Gaddafi focus and targeted Libyan government interests. Others, such as Abu al-Faraj al-Libi, who was arrested in Pakistan in 2005, became aligned with bin Laden and are believed to be part of the Al-Qaeda (AQ) leadership structure. On 3 November 2007, AQ leader Ayman al-Zawahiri announced a formal merger between AQ and LIFG. However, on 3 July 2009, LIFG members in the UK released a statement formally disavowing any association with

AQ. In September 2009, six imprisoned LIFG members issued a 417-page document that renounced violence. More than 100 LIFG members pledged to adhere to this revised doctrine and have been pardoned and released from prison in Libya since September 2009. LIFG has been largely inactive operationally in Libya since the late 1990s when members fled predominately to Europe and the Middle East because of tightened Libyan security measures. In early 2011, in the wake of the Libyan revolution and the fall of Gaddafi, LIFG members created the LIFG successor group, the Libyan Islamic Movement for Change (LIMC), and became one of many rebel groups united under the umbrella of the opposition leadership known as the Transitional National Council. Former LIFG emir and LIMC leader Abdel Hakim Bil-Hajj was appointed the Libyan Transitional Council's Tripoli military commander during the Libyan uprisings and has denied any link between his group and AQ.

Morocco

The Moroccan royal family dates its ancestry back almost 500 years and took power upon independence in 1956 after periods of interest by Spain and then France. The current monarch is King Mohammed VI. Morocco also exercises de facto administrative control in Western Sahara and enjoys a moderately free press, but the government has taken action against journalists who they perceive to be challenging the monarchy, Islam or the status of Western Sahara. Influenced by protests elsewhere in the region, and then in Morocco, King Mohammed VI responded with a reform programme. In 2012 the Justice and Development Party, a moderate Islamist party, won the largest number of seats, in the newly called for elections, becoming the first Islamist party to lead the Moroccan Government. Money laundering is a concern due to Morocco's international narcotics trade, vast informal sector, trafficking in persons, and large level of remittances from Moroccans living abroad. Cash-based transactions in connection with Morocco's substantial trade in cannabis are of particular concern. Criminal activities of risk include bulk cash smuggling and trade-based money laundering, including invoice fraud and the purchase of smuggled goods.

Moroccan Islamic Combatant Group (GICM) - Morocco

Designated as a Foreign Terrorist Organisation on 11 October 2005, the Moroccan Islamic Combatant Group (GICM) is a transnational terrorist group centred in the Moroccan diaspora communities of Western Europe. Its goals include establishing an Islamic state in Morocco. The group emerged in the 1990s and is composed of Moroccan recruits who trained in armed camps in Afghanistan, including some who fought in the Soviet war in Afghanistan. GICM members interact with other North African extremists, particularly in Europe. GICM members are believed to be among those responsible

for the 2004 Madrid train bombings, which killed 191 people. GICM members were also implicated in the recruitment network for Iraq, and at least one GICM member carried out a suicide attack against coalition forces in Iraq. According to open source reports, GICM individuals are believed to have participated in the 2003 Casablanca attacks. However, the group has largely been inactive since these attacks, and has not claimed responsibility for or had attacks attributed to them since the Madrid train bombings. In the past, GICM has been involved in narcotics trafficking in North Africa and Europe to fund its operations.

Tunisia

Rivalry between French and Italian interests in Tunisia culminated in a French invasion in 1881 and the creation of a protectorate. Agitation for independence in the decades after World War I was finally successful in getting the French to recognise Tunisia as an independent state in 1956. The country's first president, dominated the country for 31 years, repressing Islamic fundamentalism and establishing rights for women unmatched by any other Arab nation. In a 1987 bloodless coup, President Zine el Abidine Ben Ali took power. Whilst Islamic groups have agitated against the government, including the Tunisian Combatant Group, it was street protests that began in Tunis in December 2010 over high unemployment, corruption, widespread poverty and high food prices escalated in January 2011, that culminated in rioting with hundreds of deaths and would be the start of the Arab Spring. On 14 January 2011 Ben Ali dismissed the government and fled the country and by late January 2011, a "national unity government" was formed. Human rights activist Moncef Marzouki was elected as interim President.

Tunisian Combatant Group

The Tunisian Combatant Group (TCG) is a terrorist entity dedicated to the creation of an Islamic state in Tunisia. They are loosely organised and operate in small cells in Afghanistan and Western Europe. They target Tunisian interests as well as attacking Western targets and those of the US. TCG is nominally committed to a fairly specific objective, namely the creation of an Islamic state in Tunisia. However, members have been linked to Al-Qaeda and radical Islamist network in Western Europe that support Al-Qaeda and other terrorist operations. The Tunisian Combatant Group has assisted in recruiting, logistics, and the falsification of documents for the jihadist network in Europe. In addition to its ties to Al-Qaeda, TCG members are also associated with the Salafist Group for Preaching and Combat (GSPC). In December 2001, TCG's co-founder was arrested in Belgium for providing falsified documents to terrorists. In 2002, an Italian court sentenced several Tunisian Combatant Group members. These were the first convictions of Al-Qaeda associates in Europe following the September 11, 2001 attacks.

Special Focus 1

Al-Qaeda in the Islamic Maghreb (AQIM)



The Salafist Group for Call and Combat (GSPC) was already designated in the US as a Foreign Terrorist Organisation on March 27, 2002, but after the GSPC officially merged with Al-Qaeda (AQ) in September 2006 and became known as Al-Qaeda in the Islamic Maghreb (AQIM). AQIM

remains largely a regionally-focused terrorist group. It has adopted a more anti-Western rhetoric and ideology and has aspirations of overthrowing "apostate" African regimes and creating an Islamic Caliphate. AQIM factions in the northern Sahel (northern Mali, Niger, and Mauritania) conducted kidnap for ransom operations and conducted small-scale attacks and ambushes on security forces. The targets for kidnap for ransom are usually Western citizens from governments or third parties that have established a pattern of making concessions in the form of ransom payments for the release of individuals in custody.

In September 2010, AQIM claimed responsibility for the kidnapping of seven people working at a mine in Niger. AQIM released three of the hostages in February 2011, but at year's end, four French citizens remained in captivity. AQIM continued kidnapping operations throughout 2011. In January, AQIM kidnapped two French civilians in Niamey, Niger. The kidnappers later killed both hostages during a failed rescue attempt. In February, AQIM conducted its first abduction of a foreigner in Algeria since 2003 when it kidnapped an Italian tourist in Alidena. In October, AQIM kidnapped two Spanish and one Italian aid worker from a refugee camp near Tindouf, Algeria. In November, AQIM was responsible for the November 26 killing of a German man in Mali and the abduction of three men from the Netherlands, South Africa, and Sweden in Mali. AQIM members engage in kidnapping for ransom and criminal activities to finance their operations. Algerian expatriates and AQIM supporters abroad, many residing in Western Europe, provide limited financial and logistical support.

In 2013 AQIM took more than 800 hostages in a remote Gas facility in Algeria. After a tense stand-off, the crises ended with 40 hostages and 29 combatants dead. Counter terrorism pressure has pushed AQIM into the Sahara-Sahel and kidnapping and smuggling have become the most popular ways of raising finance as shown by one of Mokhtar Belmokhtar's many nom

de guerre : 'Mr Marlborough', a reference to his cigarette smuggling activities. It was he who led the splinter faction called the Islamist al Muthameen (Masked) Brigade or al Mu'aq'i'oon (those who sign with Blood) Brigade who attacked the gas facility. However, according to David Benjamin former Ambassador at Large and co-ordinator for counterterrorism at the US State Department and John Filiu Professor of Middle East Studies at Sciences Po in Paris in an article for the Center for Strategic and International Studies they believe that "There is no grand strategy of global jihadi expansion from North Africa and the Sahel. According to Filiu rising violence associated with Al-Qaeda in the Islamic Maghreb (AQIM) is instead fuelled by competition and escalation between various fragmented groups in the region. Daniel Benjamin agreed that militant activity in the region is focused locally, rather than globally and that the range of jihadist groups in the Maghreb and Sahel are fragmented, in conflict with one another, and ultimately defined by "gangsterism". Filiu argues that the various leaders within and without AQIM argue over tactics and territory. AQIM is still mainly an Algerian organisation notwithstanding Al-Qaeda's input and many militants from North Africa prefer to fight in Syria perceiving clearer and cleaner ideology. There is a clear link between jihadist and criminal activity and the groups are little more than "desert gangsters with little or no education" says Filiu.

The most sophisticated jihadi group in the region was the Libyan Islamic Fighting Group, which rejected Al-Qaeda's doctrines. Benjamin points out that AQIM activity for the past five years has been predominantly criminal rather than promoting jihad. A French official in charge of combatting terrorist finance suggests that "AQIM no longer relies on crime to finance terrorism. Now terrorism is used as a cover up for crime the sole purpose of which is to make a fortune." Filiu argues that the French governmental intervention in Mali was successful but AQIM and others in the region still demonstrate their ability to continue perpetrating attacks such as the January 2013 attack on the Gas facility in Algeria. Benjamin notes that the new regional norm will be one in which foreign governments and companies cannot rely on local governments to protect them. He suggests that the threat of North African jihadists will continue to be "a persistent but non-existent threat to regional and global security" also suggesting that it will not pose a security threat similar to that posed by the Federally Administered Tribal Areas (FATA) in Pakistan. Both agreed that development of real democracy is still the best antidote to jihadism across the region, with Benjamin adding that economic catastrophe, more than ideological radicalization, is most likely to bring new recruits to these groups.

A splinter group, the Movement for Oneness and Jihad in West Africa broke with AQIM in 2011.

West Africa



West Africa, is the westernmost region of the African continent, south and West of the Maghreb and North and West of Central Africa. West Africa includes, Burkina Faso and Niger which are mostly in the Sahel, a transition zone between the Sahara desert and the Savanna as well as Benin,

Côte d'Ivoire, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Senegal, Sierra Leone, Togo, and Nigeria. The area also includes Cape Verde, an island country in the Atlantic Ocean. All these countries are members of the Economic Community of West African States (ECOWAS) set up in May 1975. In contrast to most of Southern and Central Africa, West Africa is not populated by Bantu-speaking peoples.

Islam is the predominant religion of the West African interior and the far west coast of the continent. Traditional Muslim areas include parts of Senegal, Gambia, Mali, Guinea, Niger; the inland areas of Sierra Leone and Liberia; the western, northern and far-eastern regions of Burkina Faso; and the northern halves of the coastal nations of Cameroon, Nigeria, Benin, Togo, Ghana and Ivory Coast. The rest is mainly considered as following Christianity, though each of Islam and Christianity in the region mixes with traditional African religious traditions including voodoo.

The history of West Africa includes settlers from the empires of the Mediterranean and trade by sea and across the deserts with the North following the domestication of the camel. Much later the region became a centre for the European slave trade, with settlements along the coast being established by first Portuguese, the French and the English. In the early 19th century, Britain controlled the Gambia, Sierra Leone, Ghana, and Nigeria throughout the colonial era, while France unified Senegal, Guinea, Mali, Burkina Faso, Benin, Ivory Coast and Niger into French West Africa. Portugal founded the colony of Guinea-Bissau. Following World War II, nationalist movements arose across West Africa. In 1957, Ghana became the first sub-Saharan colony to achieve its independence. By 1974, West Africa's nations were entirely autonomous. Since independence, many West African nations have been submerged under political instability, with notable civil wars in Nigeria, Sierra Leone, Liberia, and Ivory Coast, and a succession of military coups in Ghana and Burkina Faso.

Much of West Africa suffers from endemic corruption, weak law enforcement and the informal cash-based economy provide a fertile environment for other illegal

activities that are predicate offenses for money laundering. There is an extensive black market for smuggled goods and in diamond producing countries such as Sierra Leone, a problem of smuggling diamonds and precious metals in the region.

The regional giant is Nigeria, with its vast oil wealth, a population that includes one in every five Africans and a willingness to get involved into regional conflicts have made the country a power in West Africa and a political force across the continent. Nigeria is the region's largest economy representing 55% of West Africa's gross domestic product, the most populous nation on the continent at an estimated 130 million people and the continent's largest oil producer. Nigeria played a pivotal role in founding the Economic Community of West African States, or ECOWAS, in 1975 as a regional economic organisation of 15 member countries

Nigeria

The English-speaking Republic of Nigeria in the Western part of Africa surrounded by French speaking Chad, Benin, Cameroon and Niger and with a population of 160 million in terms of size and population is the largest country in sub-Saharan Africa. Nigeria received in 1914 its name and final geographical entity when the British amalgamated the former Protectorates of Northern Muslim and Southern Christian Nigeria. The country became independent in 1960. During the over 50 years of independence repeated military interventions led to political instability and endemic corruption. From 1999 when the military finally handed over power soon after the death of Sani Abacha, one of the most corrupt leaders in history to a democratically elected government headed by Olusegun Obasanjo the fight against corruption has been made a top priority of each democratic government, though progress has been made real concerns remain. Still, certain top public officials whilst in office benefit from immunity from prosecution which hinders the fight against corruption as does the lack of any transparency of income and wealth for these and other public officials, though this is not exceptional and applies to many countries and not just Nigeria. Estimates of revenues lost through corruption vary, though most agree that the figures are likely to be in the tens of billions of US\$, and whilst some seek to bank these illicit funds in offshore bank accounts it is considered more likely that the funds will be converted and used to acquire properties, luxury cars and shares in blue chip companies, amongst other things. According to Transparency International, Nigeria ranks 144 out of 175 in its 2013 Corruption Perception Index.

The divide between North and South is increasingly marked with the differences in religion between Muslims and Christians exacerbated by terrorist groups such as Boko Haram and between rich and poor and the wealth generated out of the Oil in the Niger Delta little of which benefits the locals and the environmental

damage that is also prevalent and is the main complaint of MEND the Movement for the Emancipation of the Niger Delta. Nigeria is a leading petroleum producer and exporter, the 11th largest producer of petroleum in the world and ranked 10th, and 8th respectively for proven petroleum and natural gas reserves. It is the most important economic power of West Africa, producing approximately 50% of the regional GDP. To try to address the North South divide, there is a convention that requires the Nigerian Presidency to rotate between a member of the Muslim north and the Christian south. Current President is Goodluck Jonathan a Christian from the south and former vice president under President Yar'Adua, a Muslim from the North who died in May 2010.

Nigerian Crime Gangs

Whilst domestic crime is also a problem, Nigerian criminal gangs are also active internationally. While Nigerian organised crime networks are a relatively new phenomenon, they have nonetheless grown quickly in size and influence. The rise of Nigerian crime syndicates has been aided by the region's political corruption and instability, alongside economic setbacks such as the oil crisis of the 1980s. The large Nigerian diaspora community is a further supporting factor in the ascendancy of crime gangs from this area, who find at their disposal a readily accessible recruitment pool in many foreign states. At present no consensus exists as to the definite organisational structure of the Nigerian crime groups; some believing them to be modelled on western mafia-like hierarchies, while others perceive them to be organised around the cohesion of small independent groups. Less contested is the ethnic and tribal dimension that can be seen to run through the Nigerian crime groups. In terms of activity, Nigerian gangs are known to participate in drug trafficking, forgery, counterfeiting, money laundering and human trafficking, particularly in conjunction with the sex trade. They are particularly famed for their identity scams. As a result of the activity of these groups Nigeria, despite producing only small drug quantities, has become a hub for the transportation of heroine and cocaine. Nigerian crime networks are known to have links with other groups of international influence, such as the Colombian cartels and African American drug dealers.³ Beyond their own state, the territories of direct Nigerian operation include West African countries, South Africa, the UK, France, Belgium, Spain, Italy, the Netherlands and Greece.

Nigerian crime groups are also known to operate as far afield as the US, South America and Australia. Nigerian crime groups have become so well known for their financial scams that a diverse range of fraud transactions are referred to simply as Nigerian or 419 scams (indicating the article of Nigerian law that prohibits them). The Nigerian 419 scam is a deception technique whose lineage can be traced back into the sixteenth century with the emergence of the Spanish Prisoner Letter. This original ruse told the tale of a wealthy man incarcerated

in Spain, who required a small sum of money to be paid to prison guards as bribes. On release the wealthy former prisoner would return the funds of his kind benefactor, alongside a healthy return. This would of course never happen and the original sum paid would be lost. While the medium of communication has changed somewhat from the days when letters might be received from imprisoned noblemen, the content of the messages has changed little over the centuries. Similar language techniques are used to create trust and the portrayed circumstances are informed by current events to increase their plausibility; commonly e-mails are received from businessmen purportedly seeking to transfer funds out of an unstable zone recently featured in news coverage. E-mail technology has allowed fraudsters to reach millions of people across the world, and while the majority do not respond to their requests, a very small minority are convinced and consequently fall victim to this form of fraud.

The Movement for the Emancipation of the Niger Delta (MEND) - Nigeria

MEND is a terrorist group that uses violent means to support the rights of the ethnic Ijaw people in the Niger Delta. In contrast to the healthy profit margins enjoyed by foreign oil companies most Nigerians in the Delta region live in poverty. These conditions have led to the proliferation of local terrorist groups numbering around 120. Of these organisations, MEND is one of the largest, and it works closely with other militant groups. Notably, the Niger Delta People's Volunteer Force (NDPVF), the Coalition for Militant Action in the Niger Delta, and the Martyrs' Brigade. Led by a notoriously shadowy and secretive elite cadre, MEND's ultimate goal is to expel foreign oil companies and Nigerians not indigenous to the Delta region from Ijaw land. In the short run, the group wishes to increase local control over money made from the exploitation of the region's abundant natural resources. For instance, the organisation recently pressured the government to demand the payment of US\$1.5billion from Shell Oil for damage done to the local environment. MEND also wants the central government to provide basic services such as running water to the region and increase government investment in the area's infrastructure. Finally, MEND wishes to secure the release of imprisoned Ijaw advocates Alhaji Dokubo-Asari, a leader of NDPVF, and Diepreye Alamieyeseigha, the former governor of Bayelsa State. MEND's tactics have evolved from crude kidnapping-for-ransom operations into more sophisticated and effective methods that combine actions such as hostage-taking and bombings with the effective use of local and increasingly international media propaganda campaigns. MEND bombings usually target key points in oil pipelines and facilities in the Delta to maximize disruption and cost to foreign oil companies. In February 2006 MEND issued a declaration of "total war"³ on foreign oil and the subsequent "dark February" campaign of violence.⁴

Special Focus 2

Boko Haram - Nigeria



The group Jama'atu Ahlis Sunna Lidd'awati wal-Jihad, known better as Boko Haram, is an extremist Islamic sect in Nigeria that has created havoc across the north of the country and in the capital, Abuja. Its violent attacks on government offices, the UN, and Christian churches

threaten to destabilize the country. Since August 2011 Boko Haram has planted bombs almost weekly in public or in churches in Nigeria's northeast. Formed in 2002 the organisation is motivated by its desire to establish an Islamic state in place of the current democratic government and to eradicate all Western influences in Nigerian society. Even activities broadly associated with the West are prohibited by the group, including voting in elections and receiving a secular education. This last prohibition has led the group to target the Nigerian education system and initiate a campaign of arson against schools.⁵

In March 2012, 12 public schools in Maiduguri were burned down during the night, and as many as 10,000 pupils were forced out of education.⁴ Boko Haram has also become infamous for its deployment of gunmen mounted on motorbikes, commonly used to eliminate prominent opposition figures in swift attacks. Historically, the group can trace its origins to the Sokoto Caliphate. Formerly one of sub-Saharan Africa's leading empires the Islamic Sokoto Caliphate spanned parts of northern Nigeria, Niger and southern Cameroon from 1809-1903, when it was conquered by the British. Throughout the colonial period and following independence the Muslims of this geographical and spiritual community have strongly resisted Western influence. The reclamation of the Soko Caliphate territories remains Boko Haram's objective and the communities located in these areas continue to be their main support base. In 2011 the organisation was brought to the attention of the international community as a result of multiple bombings, including the 2011 Christmas Day bombings on the outskirts of Nigeria's capital. A US Congressional Report published in the same year described Boko Haram as an emerging threat and speculated that the group may be forming links with Al-Qaeda. In February of 2012 information surrounding the funding of Boko Haram emerged from a Nigerian state security investigation. According to the findings of this investigation the group relied on a combination of member donations, however support from the terrorist group Al-Qaeda in the Islamic Maghreb (AQIM) later allowed the group to channel revenue from further

afeld. Consequently funding is believed to have been received from support groups in Saudi Arabia and the UK. Also amongst the investigations findings are alleged financial links between Boko Haram and an Islamic society based in Saudi Arabia. Boko Haram remains operative in Nigeria and is considered a threat to both Nigerian citizens and foreign nationals. Ansaru or the Vanguard for the Protection of Muslims in Black Lands is an Islamist jihadist organisation based in the northeast of Nigeria. Whilst it is an offshoot of Boko Haram founded in 2012, it is less aggressive to non-muslims than Boko Haram and is thought to have a more international focus.

Area Boys (Agberos) - Nigeria

A loosely organised group of teenagers and abandoned youth that roam the streets of Lagos, Nigeria this group has been known for its practices of extortion and drug violence. One of the methods the groups use for extortion is to surround pedestrians, drivers and passengers in vehicles, which are stuck in traffic, and force them to pay before letting them go. Area Boys, who are largely "Yoruba" have existed in the city since the 1980s, however they can trace their origins back to the 1920s. In 2007 the number of Area Boys in Lagos was estimated at over 35,000.

Sierra Leone

The history of Sierra Leone as an independent nation began in 1961, though the lands had been inhabited since at least 2,500 years ago. Sierra Leone began as a colony of freed British slaves. Recent history has been dominated by the eleven year war which lasted from 1991 until 2002, which was characterized by extreme brutality and widespread human rights abuses against civilians. The majority of the crimes were perpetrated by rebels from the Armed Forces Revolutionary Council (AFRC) and the Revolutionary United Front (RUF). However, government forces and their allies, notably the Civil Defense Forces (CDF), also committed serious crimes, albeit on a smaller scale and of a different nature than those by rebel groups. During the conflict, tens of thousands of civilians were killed and up to one-quarter of the population was displaced. During the war, rebels, and to a lesser extent government forces, consistently failed to distinguish between civilians and combatants. Hundreds of civilians suffered from the signature rebel atrocity of limb amputation while thousands of girls and women were subjected to sexual violence. All sides recruited and used child combatants. Sierra Leone, particularly via its large seaport and porous borders, together with pervasive corruption make it conducive to money laundering, for illegal drugs or other forms of illegal commerce, for example the smuggling of pharmaceuticals, foodstuffs, gold, and diamonds. Transactions at most levels, money exchanges, and remittances are very informal and based on cash and vulnerable to money laundering.

Revolutionary United Front - Sierra Leone

The Revolutionary United Front (RUF) was a rebel army that fought a failed eleven-year war in Sierra Leone, starting in 1991 and ending in 2002. It later developed into a political party, which existed until 2007. The three most senior surviving leaders were convicted in February 2009 of war crimes and crimes against humanity. The Revolutionary United Front initially coalesced as a group of Sierra Leoneans which led National Patriotic Front of Liberia elements across the border in an attempt to replicate Charles Taylor's earlier success in toppling the Liberian government. The RUF was created with substantial assistance from Charles Taylor of Liberia and from Libya when in 1988 a group of 25-50 Sierra Leoneans travelled to Libya and received training under the Muammar Gaddafi regime.

At first, the RUF was popular with Sierra Leoneans, many of whom resented a Freetown elite seen as corrupt and looked forward to promised free education and health care and equitable sharing of diamond revenues. However, the RUF developed a reputation internationally for enormous cruelty during its decade-long struggle and resources itself from diamond mines in territory under its control. The cruelty included recruiting child soldiers, some forced to kill their parents, and using machetes, RUF rebels amputated the hands, arms, and legs of tens of thousands of Sierra Leoneans, the reason for these actions was that amputees could no longer mine diamonds, which might be used to support government troops, or fire weapons against them. Sierra Leone's economy collapsed, with ordinary citizens trapped between the cruelty of RUF troops and starvation. It became notorious for its use of child soldiers, many of whom it kidnapped and conscripted, often forcing the children to inject cocaine before sending them off to fight. The RUF continued to fight the multiple successive governments of Sierra Leone through the 1990s and, with support from Charles Taylor, intermittently occupied the diamond-producing areas of Sierra Leone, contributing to the "blood diamond" trade of West Africa.

The RUF began to suffer major setbacks when Executive Outcomes (EO), a private security firm hired by the Sierra Leonean government, pushed the rebel group back from the capital, Freetown. After this, RUF announced a cease-fire and accepted peace talks with President Kabbah, which broke down and the fighting resumed. The RUF intensified its attacks, which first brought in a Nigerian-led West African force in 1998 to combat them and later in 2000, a British intervention finally secured the country for UN supervision. Disarmament of RUF rebels began in May 2001, and the war was officially declared over in January 2002, essentially the end of the RUF. The leader of the RUF Foday Sankoh died in prison in July 2003 while awaiting trial on charges of war crimes. The war is estimated to have cost the lives of 200,000 people.

Liberia

Liberia was established in the Nineteenth century as a settlement of freed slaves from the US. In 1980, a military coup led by Samuel Doe ushered in a decade of authoritarian rule and in 1989, the Liberian civil war broke out when the National Patriotic Front of Liberia (NPFL), led by Charles Taylor, invaded the country to oust the Liberian dictator. The NPFL soon assassinated Doe and Taylor became President. At the onset of the civil war in Sierra Leone, the Taylor-backed Revolutionary United Front (RUF) joined the war and would be later accused of fueling the conflict and indicted on charges of war crimes. Taylor under immense pressure and invasions from opposition groups left Liberia in 2003. After two years of rule by a transitional government, democratic elections in late 2005 brought President Ellen Johnson Sirleaf to power, who was also re-elected in 2011. The Liberian economy is essentially cash-based, with both Liberian and US dollars being legal tender, facilitating the laundering of US currency. Liberia has a significant market for smuggled goods, which are easily imported through its porous borders.

Mali

Mali, arose in its current form following the break up of French Colonies in West Africa in 1960. Rule by dictatorship was brought to a close in 1991 by a military coup that ushered in a period of democratic rule. Former President Amadou Toure was elected to a second term in 2007 in elections that were widely judged to be free and fair. Malian returnees from Libya in 2011 exacerbated tensions in northern Mali, and Tuareg ethnic militias including Ansar Dine, started a rebellion in January 2012, leading to the downfall of the President. The Chaos that followed led to initial Islamic success in taking control of Northern regions but these have been retaken by the military and since August of 2013, Ibrahim Boubacar Keita was elected president. Illegal proceeds in Mali derive from rampant trafficking of drugs, small arms, people, and everyday commodities across the Algerian, Nigerian and Mauritanian borders in the sparsely-populated north of the country. Authorities believe terrorist cells from Al-Qaeda in the Islamic Maghreb, known to operate in the north, are involved in smuggling as well as kidnapping for ransom to generate funds. The majority of Mali's economy is cash-based, making it difficult to track illegal or criminal financial transactions. Malian authorities believe proceeds being returned to South America from cocaine trafficking in Europe may be passed through Malian banks.

Ansar Dine - Mali

Ansar Dine means "helpers of the Islamic Religion" or "defenders of the faith" and is a militant Tuareg group with ties to AQIM with ambitions to impose Islamic law across Mali.

The Horn of Africa



The Horn of Africa (alternatively Northeast Africa or Somali Peninsula) is a peninsula in East Africa that juts hundreds of kilometers into the Arabian Sea and lies along the southern side of the Gulf of Aden. It is the easternmost projection of the African continent.

Referred to in ancient and medieval times as Bilad al-Barbar ("Land of the Barbarians"), the Horn of Africa denotes the region containing the countries of Eritrea, Djibouti, Ethiopia and Somalia.

Djibouti

The French Territory of the Afars and the Issas became Djibouti in 1977. A Somali Issa dominated authoritarian government ruled until 1999, during which unrest among the Afar minority led to a civil war that finally ended in 2001 with a peace accord between the two sides. In 1999, Djibouti's first multiparty presidential elections resulted in the election of Ismail Omar Guelleh, who continues to rule today as President in his third term. Djibouti is today one of the most stable countries in the Horn of Africa, occupying a strategic geographic location at the intersection of the Red Sea and the Gulf of Aden and serves as an important shipping lane for goods entering and leaving the east African highlands and transshipments between Europe, the Middle East, and Asia. The government holds long-standing ties to France, which maintains a significant military presence in the country, and has strong ties with the US.

There are also allegations of some financial facilitation for Somali based Al-Shabaab and involvement in the laundering of some Somali ransom payments derived from piracy. Smuggled goods include high taxed cigarettes and alcohol. Djibouti is a transit, source, and destination country for men, women, and children subjected to forced labour and sex trafficking. Economic migrants from East Africa en route to Yemen and other Middle East locations are also vulnerable to exploitation in Djibouti.

Eritrea

The UN established Eritrea as an autonomous region within the Ethiopian federation in 1952. Ethiopia's full annexation of Eritrea as a province 10 years later sparked a violent 30-year struggle for independence that

ended in 1991 with Eritrean rebels defeating Ethiopian government forces. Eritreans overwhelmingly approved independence in a 1993 referendum. Isaias Afeworki is considered highly autocratic and repressive, ruling as President since independence.

There are concerns that the Eritrean government and military officials profit from contraband smuggling and extortion. Due to its informal cash economy, underground remittances and the prevalent use of money/value transfer systems, alongside proximity to regions where terrorist and criminal organisations operate, and widespread corruption Eritrea make this combination of concern. Eritrea is believed to have been a haven for organisations affiliated with Al-Qaeda and Al-Shabaab, with some considering that elements of the Eritrean security apparatus provide training, supplies and financing to regional destabilisers, indeed past support to insurgents in neighboring states resulted in the UN Security Council (UNSC) levying an arms embargo against Eritrea in 2009. By 2012, the UN concluded that Eritrea had reduced or eliminated direct support for Al-Shabaab, but recommended maintaining the existing arms embargo until greater transparency is achieved. Eritrea is a source country for men, women, and children subjected to forced labour and, to a lesser extent, sex trafficking.

Ethiopia

Ethiopia has the distinction, among African countries, of largely avoiding European colonial rule, with the exception of a short-lived Italian occupation from 1936-41. In 1974, a military junta, the Derg, deposed Emperor Haile Selassie, (who had ruled since 1930) and established a socialist state. Torn by bloody coups, uprisings, wide-scale drought, and massive refugee problems, the regime was finally toppled in 1991 by a coalition of rebel forces, the Ethiopian People's Revolutionary Democratic Front (EPRDF). A border war with Eritrea late in the 1990s ended with a peace treaty in December 2000. In 2007 Ethiopian forces invaded southern Somalia to stop the rise of the Council of Islamist Courts routing them from Mogadishu and elsewhere in Somalia.

Ethiopia's location within the Horn of Africa makes it vulnerable to money laundering-related activities perpetrated by transnational criminal organisations, terrorists, and narcotics trafficking organisations. Sources of illegal proceeds include corruption, smuggling, and trafficking in narcotics, persons, arms, and animal products. Ethiopia is a transit hub for heroin originating in Southwest and Southeast Asia and destined for Europe, as well as cocaine destined for markets in southern Africa; Khat is cultivated for local use and regional export, principally to Djibouti and Somalia (legal in all three countries). High tariffs encourage customs fraud and trade-related money laundering. Law enforcement sources indicate money and value transfer systems, particularly hawala, are widely used.

Somalia

Both British and Italian Somaliland joined together in 1960 to form the new nation of Somalia. In 1969, a coup ushered in an authoritarian socialist rule. After the regime's collapse early in 1991, Somalia descended into turmoil, factional fighting, and anarchy.

In May 1991, northern clans declared an independent Republic of Somaliland. Although not recognised by any government, this entity has maintained a stable existence and continues efforts to establish a constitutional democracy, including holding municipal, parliamentary, and presidential elections. Another region, known as Puntland has become a semi-autonomous state which has been self-governing since 1998.

In the meantime the rest of Somalia since 1991 has suffered from major internal strife, famine and civil war with warlords ruling areas and little central government control leading to it being considered for much of the time as a failed state. In 2000, a peace agreement resulted in the formation of an interim government, known as the Transitional National Government (TNG), which was succeeded in 2004 by the Transitional Federal Government (TFG). Both governments faced constant opposition from Islamic Somali militant groups. For example, Al-Ittihad al-Islamiya co-operated with Al-Qaeda operators who carried out the [1988 US Embassy Bombings](#) in East Africa. The Group was succeeded by the Council of Islamic Courts that made major territorial gains against the TFG including the capture of the capital Mogadishu. Ethiopian forces responded invading southern Somalia and routing the Council of Islamist Courts in 2007, leaving once the TFG had been re-established in 2009. Recent elections in 2012 have been widely hailed as a great success, with Hassan Sheikh Mohamud, a moderate Muslim, emerging as the country's new leader. The Somali National Army forces, alongside troops from the African Union Mission in Somalia, have continued to combat the successor group to the Council of Islamic Courts, known as Al-Shabaab, making significant gains against the terrorist group, pushing the extremist militia out of all major cities it previously held.

Nevertheless the influence of Al-Shabaab has not been dispelled from Somalia, nor from its effects on its neighbors particularly in Kenya. Somalia does not have a formal financial system, and the majority of financial entities operating in Somalia, such as money transmitters and hawaladars, are not supervised or monitored by regulatory or enforcement agencies. Smuggling is rampant. Somalia has one of the longest land borders as well as the longest coastline in Africa. Public and private sector corruption, remains a significant concern, with Somalia ranking 175 of 175 countries on Transparency International's 2013 Corruption Perception Index. Although acts of piracy off the coast of Somalia have de-

creased significantly over the past 18 months, proceeds from ransom payments still contribute to Somalia's illicit activity. The ransoms are delivered through cash drops to pirates holding ships off Somalia's coast. They are divided among the pirates themselves, their support networks on shore, and possibly national and international sponsors. Much of the ransom reportedly remains in cash.

Special Focus 3 Al-Shabaab - Somalia



Al-Shabaab, or 'the youth', is the name generally applied to the Somali militant group which was formerly the most prominent of the militia groups comprising the militant wing of the Council of Islamic Courts (CIC), itself a successor organisation of Al-Ittihad al-Islamiya. Al-Ittihad was

associated with bin Laden and co-operated with Al-Qaeda operators who carried out the [1988 US Embassy Bombings](#) in East Africa. The group, which proclaims its intention to establish an Islamic state encompassing the Muslim dominated territories of Somalia, Somaliland, Puntland, north-eastern Kenya, the Ogaden region of Ethiopia and Djibouti, has, since the TFG's seizure of power, conducted violent insurgency against government targets. Al-Shabaab has also pledged to eliminate the influence and presence of foreign 'infidels'. In terms of organisation, the group is based around the allegiance and coherence of a number of regional leaders, many of whom led very distinct factions. Estimates of the group's size range from 3,000 to 7,000 members, the bulk of which are drawn from Somalia. The group is known to have links with Al-Qaeda, to whom Al-Shabaab leader Mukhtar Abu al-Zubair has publicly pledged allegiance. In January 2013 Al-Shabaab targeted the Somali presidential palace with a suicide bombing. The most recent attack in September 2013 in a [Nairobi Shopping Centre](#) provides ample evidence that Al-Shabaab continues to pose a very real threat in Somalia and with its neighbours posing a threat beyond its borders and is a concern for security experts in large part due to a significant far flung diaspora, including 2 million in America (especially Minnesota), in the UK (London and Cardiff), Scandinavia and Kenya, concerned that some may pose direct threats as an Al-Qaeda affiliate in these Countries and/or in recruitment of Al-Shabaab volunteers and as a source for financing. Al-Shabaab also receives financing from multiple sources, mainly from the illicit trade in charcoal from its controlled territories.

Eastern Africa



Eastern Africa comprises at its core the three countries of Kenya, Tanzania and Uganda. Whilst some other countries could be included, they nevertheless can be better placed in the Horn of Africa, for example Djibouti, Eritrea, Ethiopia, and Somalia, or in Central Africa in the

case of Burundi and Rwanda, with Mozambique which can be considered part of Southern Africa. That leaves Sudan and South Sudan, Comoros, Madagascar, Malawi, Mayotte, Mauritius, Réunion and Seychelles as part of Eastern Africa.

East Africa is according to conventional wisdom, the origin of modern humans, who left East Africa to migrate all over the world. Between 2500–3000 years ago, Bantu-speaking peoples began a millennia-long series of migrations eastward from their homeland that is (modernly known as) southern Cameroon across the Rwenzori Mountains. This Bantu expansion introduced agriculture into those parts of East Africa either not reached previously by Nilo-Saharan farmers or too wet for millet. During the following fifteen centuries, the Bantu slowly intensified farming and grazing over all suitable regions of East Africa, in the process making contact with Austronesian- and Arabic-speaking sailors on the southern coastal areas. The latter also spread Islam to the coastal belt, but most Bantu never had contact with Islam and remained animists. The Bantu expansion was followed by the Nilotic expansion across parts of East Africa during the 14th to 18th centuries.

Sudan

The Sudan is located in Northeastern Africa and it is the largest country in Africa. It is also the tenth largest country in the world based on area. Sudan is not part of Sub Saharan Africa as the Sahara technically starts to the West of Sudan and is more accurately described as either part of the Nile river delta or instead great East Africa. Sudan has a long history of civil wars as well as political and social instability. Most recently Sudan split when South Sudan, mainly Christian seceded from mainly Muslim Sudan in 2011, following a decades long Civil war.

Sudan has a long history that begins with its being a collection of small kingdoms until Egypt conquered the area in the early 1800s. At this time however, Egypt only controlled the northern portions, while the south was made up of independent tribes. In 1881, Muham-

mad ibn Abdalla, also known as Mahdi, began a crusade to unify western and central Sudan which created the Umma Party. In 1885, the Mahdi led a revolt but he died soon after and in 1898, Egypt and the UK regained joint control of the area, until Independence was gained in 1956. Sudan's first leaders began to renege on promises to create a federal system which began a long period of civil war in the country between the northern and southern areas as the north has long tried to implement Muslim policies and customs. [The Sudan People's Liberation Army](#) fought against the government throughout this time.

A second separate conflict, has led to genocide charges being brought against the current President of Sudan, Omar Bashir. The conflict which broke out in the Western region of Sudan known as Darfur in 2003, which is home to about 6 million people and is about the size of France. Darfur is home to racially mixed tribes of settled peasants, who identify as African, and nomadic herders, who identify as Arab. The majority of people in both groups are Muslim. The African groups, after suffering years of government sponsored neglect and racism launched an uprising. The government responded by implementing their campaign of genocide, enlisting the help of Arab militia in Darfur called the Janjaweed. The dispute is racial, not religious: Muslim Arab Sudanese are killing Muslim black Sudanese. The Janjaweed are the armed militia supported by the Sudanese Government who carry out the genocide, alongside and independent of, the Sudanese Army. Up to 400,000 people have died due as result of direct attacks and conflict induced malnutrition and disease. The vast majority of these have been women, children and civilian men and millions have been displaced. A UN peacekeeping force is now operating in the region.

Sudan is designated by the US since 1993 a "state sponsor of terrorism," alleging it harboured local and international terrorists, including bin Laden, Hezbollah, Hamas, Palestinian Islamic Jihad, the Abu Nidal Organisation, Jamaat al-Islamiya, and Egyptian Islamic Jihad. US investigators also linked two Sudanese diplomats to a terrorist cell planning to bomb the UN building in New York. In 1998, Al-Qaeda operatives based in Sudan were allegedly involved in the [bombings of US Embassies in Kenya and Tanzania](#). Throughout the 1990s, Sudan was also accused of supporting local insurgencies in Uganda, Tunisia, Kenya, Ethiopia, and Eritrea. In 1997, the U.S. imposed comprehensive economic, trade, and financial sanctions against Sudan. In 1996, the UN Security Council placed sanctions (PDF) on Sudan for harboring suspects wanted for the attempted assassination of President Hosni Mubarak of Egypt. The UN lifted terror related sanctions in 2007 following Sudan's willingness to combat terrorism, also welcomed by the US, though US sanctions remain in part due to its continued support for Hamas. Its relationship with the US and other Western states also remains troubled because of the humanitarian crisis in Darfur, as well as US allegations that Sudan is assisting the Iraqi insur-

gency by permitting militants from Sudan and other nations to transit to Iraq.

Sudan currently has limited access to international financial markets and institutions because of comprehensive U.S. economic sanctions. Traders and other legitimate business persons often carry large sums of cash because Sudan is largely a cash-based society and electronic transfer of money outside of Sudan is challenging. This dependence on large amounts of cash complicates enforcement efforts and makes Sudan's banking system vulnerable to money laundering. Comprehensive sanctions also contribute to a significant black market for smuggled goods, making Sudan vulnerable to trade-based money laundering. Sudan is ranked 174 of 175 countries on Transparency International's 2013 Corruption Perception Index.

South Sudan

On 9 July 2011, the Republic of South Sudan became the World's newest state following the ending of the Sudanese Civil War and independence following a 2002 Agreement. Whilst the Government of Sudan was established with the support of the two largest tribes, the Dinka tribe led by President Salva Kiir, and the Nuer tribe led by former Vice President Riek Machar. With the sacking of the Vice President in July 2013 stability has been lost and violence, particularly tribal based atrocities, is leading to the outbreak of a civil war. As a result, oil production, which accounts for 98% of government revenue, had fallen by a quarter as a result of the violence and to many the real reason for the conflict.

South Sudan is not a major financial centre, and as such, there is little major financial crime; however, corruption is widespread in this oil rich state. The GOSS does not yet have significant laws, regulations, or enforcement capacity in place to address financial crimes. South Sudan has a cash-based economy. With no anti-money laundering/counter-terrorist financing (AML/CFT) regime, and its large and porous borders, South Sudan is vulnerable to exploitation by criminals of every type, including those seeking illicit routes to transport money via bulk cash smuggling and those wishing to perpetrate other forms of financial crime.

Sudan People's Liberation Army - South Sudan

The Sudan People's Liberation Army (SPLA) was formed in 1983 to oppose the implementation of sharia law, or strict Islamic law, by Sudanese President Nimeiri. While the largely Muslim population of Sudan's Northern provinces generally welcomed the change, the Christians and Animists of southern Sudan were alarmed. According to the treaty that had ended the country's first civil war in 1972, the South was to maintain its autonomy from the North. Nimeiri's attempt to implement sharia nationwide violated that agreement and created widespread resentment among the South-

ern population. Sent by the Army to quell a mutiny in the South, Lt. Col. John Garang instead embraced the insurrection and became its leader, forming the SPLA. From an initial nucleus of 500 soldiers in 1983, Garang's rebel army grew rapidly, hitting an estimated 50,000 to 60,000 by 1991. The group's stated goal was the formation of a secular, democratic Sudan. In the mid-nineties, the SPLA became the vanguard element of a rebel umbrella organisation, the National Democratic Alliance, which even contained some moderate Muslim parties. The SPLA's success, however, cost the citizens of Sudan dearly. It is estimated that the civil war, which did not cease until 2002, took some 1.5 million lives. Although the SPLA was primarily designed to perform military operations against the Sudanese Army, it also engaged in a few acts of terrorism against westerners and western interests in the country. In 1999, the SPLA took six Red Cross workers hostage, four of whom died in captivity. Although SPLA spokespeople claim that the deaths occurred during a botched rescue attempt, the Sudanese government claims that they were executed. Two years later, the SPLA claimed responsibility for one successful bombing and one unsuccessful bombing attempt against oil companies operating in Southern Sudan. The SPLA specifically targeted the oil industry to prevent oil proceeds from strengthening the government forces.

In 2002 the Khartoum government and the rebels were able to hammer out a power-sharing agreement that has ended, or at least significantly lowered the ferocity of, Sudan's civil war. As part of the implementation of this agreement, John Garang was named Vice-President of Sudan in 2004. As the SPLA has become a mainstream political force within Sudan, its interest in using terrorism as a means of achieving its goals has waned. On January 9th, 2005, the SPLA signed a peace agreement with the Khartoum regime, officially ending the Civil War that had ravaged Sudan since 1983. Under the terms of the agreement, southern Sudan would gain religious autonomy and a share of the nation's oil wealth and after a 6-year period of autonomy, residents of the South could vote on a referendum on whether to remain a part of Sudan or form an independent nation. On 9 July 2011, following the promised referendum that passed with a 98.3% of the vote, the world's newest independent State was born and is known as South Sudan.

Uganda

Uganda is a landlocked country in East Africa, bordered on the east by Kenya, on the north by South Sudan, on the west by the Democratic Republic of the Congo, on the southwest by Rwanda, and on the south by Tanzania. The southern part of the country includes a substantial portion of Lake Victoria, shared with Kenya and Tanzania. Uganda takes its name from the Buganda kingdom, which encompasses a large portion of the south of the country including the capital Kampala. Beginning in the late 1800s, the area was ruled as a colony

by the British. Uganda gained independence from Britain in 1962. The period since then has been marked by intermittent conflicts, most recently a lengthy civil war against the [Lord's Resistance Army](#), which has caused tens of thousands of casualties and displaced more than a million people. The current President of Uganda is Yoweri Kaguta Museveni, who came to power in a coup in 1986. Perhaps the most infamous figure in Ugandan recent history was that of former President Idi Amin, who came to power in a military coup in 1971. Amin ruled Uganda with the military for eight years and carried out mass killings within the country to maintain his rule. An estimated 300,000 Ugandans lost their lives at the hands of his regime, many of them in the north. Aside from his brutalities, he forcibly removed the entrepreneurial South Asian minority from Uganda, which left the country's economy in ruins. Amin's reign was ended after the Uganda-Tanzania War in 1979, in which Tanzanian forces aided by Ugandan exiles invaded Uganda.

Current President Yoweri Museveni, in power since 1986 was initially lauded by the West as part of a new generation of African leaders. As president, he has led Uganda in involvement in the civil war in the Democratic Republic of Congo (DRC) and other conflicts in the Great Lakes region. He has struggled for years in the civil war against the [Lord's Resistance Army](#), which has been guilty of numerous crimes against humanity, including child slavery and mass murder. The [Lord's Resistance Army \(LRA\)](#) seek shelter in southern Sudan and the Democratic Republic of the Congo's Garamba National Park; [LRA](#) forces have also attacked Kenyan villages across the border.

A 2012 report by the Center on Global Counterterrorism Cooperation concludes that Uganda is "deeply vulnerable to money laundering and terrorist financing" and that "money laundering is rampant in the country." Money laundering in Uganda derives largely from government corruption, misappropriation of public funds and foreign assistance, and abuse of the public procurement process. Other widespread offenses for money laundering in Uganda include arms and natural resource smuggling, exchange control violations, and human trafficking. Uganda's enormous cash-based informal economy provides a fertile environment for money laundering, as does its lack of anti-counterfeiting legislation which feeds a large black market for smuggled and/or counterfeit goods.

Lord's Resistance Army - Uganda

The militia that is today known as the Lord's Resistance Army ("LRA") was first formed in 1988 from the remnants of a defeated resistance movement amongst the Acholi people of northern Uganda. The conflict itself sprang from long-enduring ethnic tensions between the Acholi of the north and the Baganda of the south, the former fearing their marginalization by the latter. It was purportedly to continue this struggle for Acholi rights and establish a government based on the Chris-

tian faith's 10 Commandments that Joseph Kony united rebels of the Holy Spirit Movement and the Ugandan People's Democratic Army under one banner. However such intentions soon proved to be insincere and the LRA revealed itself to be driven by a personality cult centred on Kony rather than any political aspirations. Nevertheless, while the defence of Acholi rights has proved little more than a superficial justification for the armed struggle, the LRA does represent a continuation of some aspects of the former movement. For instance the LRA has adopted many of the spiritual traditions of the Holy Spirit Movement, a group also dominated by the personality of its leader and draped in a form of Christian mysticism peculiar to the region. Just as the Holy Spirit Movement's leader Lakwena expressed her messianic tendencies in the declaration that her warriors would be invincible if they rubbed themselves with shea butter, so Kony has asserted that his commands are taken from the spirit world and are therefore beyond questioning.

While the LRA at first gained support from the Acholi community located predominantly in northern Uganda, this support soon fell away amidst acts of cruelty perpetrated by the group. The organisation is renowned for its atrocities against defenceless village communities, raping, torturing and murdering indiscriminately. The abduction of young boys as a form of recruitment is also well-known, many of whom are rumoured to have been inducted in horrific rituals. Young girls are also abducted by the LRA to serve as sex slaves for the militia. Despite these atrocities, it is suspected that Kony's LRA secured the support of Omar al-Bashir's Sudanese government, who supplied the group with arms and financed their campaign in Uganda. This support however ended in 2002, a move that weakened the LRA and contributed to its retreat and dispersal into neighbouring countries.

In terms of numbers, the LRA in 2007 was estimated to have anywhere between 500 and 3,000 soldiers under its command, as well as 1,500 abducted women and children. Since then the strength of the organisation has deteriorated, with Ugandan Defence Minister Crispus Kiyonga estimating in 2012 that the LRA possessed only 200-250 active militants. These men seek refuge in the vast areas of jungle in northern Uganda and the surrounding countries, operating independently in squads of around 20 men.

Despite the LRA's reduced strength its violent activities continue; according to the LRA Crisis Tracker⁶ in January 2013: 3 civilian deaths and 13 abductions were perpetrated by the group. The LRA Crisis Tracker is maintained by an organisation that attempts to raise awareness of the humanitarian issues caused by the LRA and is the most comprehensive source of information on LRA activity publicly available. While the LRA has yet to be overcome with any degree of finality and its leader Joseph Kony remains at large, some international sanctions have been made against the group. In 2005 the International Criminal Court released arrest war-

rants for Kony and several members of the LRA senior leadership, and later Interpol supported this move by issuing red wanted notices to 184 countries for these 5 men. These notices effectively constitute an international arrest warrant, though formally the Interpol notices can only request arrest and extradition. The US has also undertaken efforts to counter the threat posed by the LRA, providing humanitarian and military support to the Ugandan government. Kony was also listed on the US Treasury Department's register of "Specially Designated Global Terrorists" in 2008, and in 2010 US President Barack Obama signed the Lord's Resistance Army Disarmament and Northern Uganda Recovery Act. This act led in 2011 to the deployment of 100 US Special Forces to the area in order to provide training and military guidance to Ugandan forces combating the LRA.⁷ In 2012 the African Union also pledged 5,000 troops to track and combat the LRA. Nevertheless the LRA and its leader Joseph Kony, though considerably weakened, remain at large and represent a considerable threat to communities in Northern Uganda and the neighbouring areas of South Sudan and the Democratic Republic of Congo.

Kenya

Kenya achieved its independence from Britain in 1963. The road to independence began in the 1950s with the Mau Mau rebellion. The Mau Mau movement was a militant African nationalist group that opposed British colonial rule and its exploitation of the native population. Mau Mau members, made up primarily of Kikuyu (the largest ethnic group in Kenya), carried out violent attacks against colonial leaders and white settlers. In 1952, the colonial government declared a state of emergency and arrested many Kenyan independence leaders, including moderates who had little or no connection to the Mau Mau, like Jomo Kenyatta, the then President of the Kenyan African Union. Whilst the British defeated the Mau Mau through a brutal campaign of military action and widespread detention of the Kikuyu, the rebellion led to reforms from which, working together with African and white Kenyan leaders, the country's transition to independence could be made. Jomo Kenyatta became the Country's first President and leading the country until his death in 1978 and as head of the Kenya African National Union (KANU). He was succeeded by President Daniel Arap Moi who ruled until 2002. The one party rule exacerbated ethnic divisions in the country and led to staggering levels of corruption. Following a campaign centered on an anticorruption platform, opposition leader Mwai Kibaki defeated KANU candidate Uhuru Kenyatta and assumed the presidency, though little was achieved in the anti corruption area once elected. By the time of the next election in 2007, widespread vote rigging concerns led to two months of violence resulting in as many as 1,500 people killed and a power-sharing accord between Kibaki and his opponent Rail Odinga.

In 2013. Uhuru Kenyatta, the son of founding president Jomo Kenyatta, won recent Presidential elections, despite being already indicted by the International Criminal Court charged with crimes against humanity, including murder, forcible population transfer and persecution, for his alleged role in the postelection violence in 2007 and early 2008. Jomo Kenyatta is also charged alongside the Deputy President William Samoei Ruto and both are also accused of responsibility for the criminal acts carried out by a criminal gang known as the Mungiki, which was allegedly under their control.

Kenya is the largest financial centre in East Africa. Kenya is a transit point for international drug traffickers. Kenya is a transit country for South Asian heroin destined for Europe and North America; Indian meths also transit on their way to South Africa. Trade-based money laundering is a problem in Kenya. There is a black market for smuggled goods in Kenya, which serves as a major transit country for Uganda, Somalia, Tanzania, Rwanda, Burundi, eastern Democratic Republic of Congo, and South Sudan. The laundering of funds derived from corruption, smuggling, illicit trade in counterfeit goods, drugs, wildlife trafficking and other financial crimes is a substantial problem. Its proximity to Somalia makes Kenya an attractive and likely destination for the laundering of piracy-related proceeds and a financial facilitation hub for Al-Shabaab. Although banks, wire services, and other formal channels execute funds transfers, there are also thriving, unregulated informal networks of hawala and other alternative remittance systems using cash-based unreported transfers. Foreign nationals, in particular the large Somali refugee population, primarily use hawala to send and receive remittances internationally. Mobile money, using telecom networks for cash transfers, is increasingly important. Kenya is a source, transit, and destination country for adults and children subjected to forced labour and sex trafficking.

Kenya ranks 136 out of 175 countries on the 2013 Transparency International Corruption Perceptions Index. Kenya is included in the October 19, 2012 Financial Action Task Force (FATF) Public Statement because it has not made sufficient progress in implementing its action plan and continues to have certain strategic anti-money laundering/counter-terrorist financing (AML/CFT) deficiencies. Kenya has been a target of terrorism, with the bombing of the US Embassy in Nairobi in 1998 when 224 died at the hands of the Egyptian Islamic Jihad and Al-Qaeda and most recently in 2013 when Al-Shabaab attacked Nairobi's Westgate Mall killing 67 people.

Mungiki - Kenya

This terrorist and organised crime gang, whose name denotes "A united people" or "multitude", began in the 1980s as a militia band based in the Kenyan highlands. The militia was formed with the purpose of protecting Kikuyu farmers from the predations of Maasai and government forces. The Mungiki arose from a social and

economic climate of deprivation and discontent. Rapid population growth resulted in mass unemployment and landlessness, with disaffected Kenyan youth finding their only sense of direction in the organised crime of the Mungiki. Effectively a conservative force in terms of its central ideology, the Mungiki gang rejects all western influence and anything believed to be tainted by the legacy of colonialism. Christianity is therefore rejected, as are many aspects of modernization that are deemed immoral or corrupting. Further anti-colonial sentiment can be detected in the Mungiki's image, which is thought to be modelled on that of the original Mau Mau fighters who violently opposed British rule.

The Mingiki first migrated to Nairobi in the 1990s, capitalising on the taxi trade, and later expanding into rubbish collection, construction, and protection services. The move to Nairobi resulted in the groups' progression from a single body to a cellular structure, with each cell containing 50 members who are then further sub-divided into platoons of 10 members. In more recent times the Mungiki have begun to play a far more prominent role in Kenya's public sphere, entering the political arena to support their favoured party. For instance during the 2002 election the Mungiki hired themselves out for the purposes of vote 'winning', and made their political allegiance with Kenya's KANU party. For around 100,000 Kenyan shillings the Mungiki could be paid to visit a neighbourhood, extracting votes by force. According to many sources an accurate estimate of the gang's size is very hard to achieve. The name Mungiki has become a brand name adopted by all those seeking to intimidate or extort, sometimes with no real connection to the gang.

Tanzania

Tanzania is a country in East Africa, bordered by Kenya and Uganda to the north; Rwanda, Burundi, and the Democratic Republic of the Congo to the west; and Zambia, Malawi, and Mozambique to the south. The country's eastern border is formed by the Indian Ocean. Kilimanjaro, Africa's highest mountain, is in northeastern Tanzania. Tanzania still includes the semi-autonomous islands of Zanzibar, and together with the mainland formerly known as Tanganyika, Tanzania merged and got its name in 1964 after it had achieved its independence from Britain and was led by President Julius Nyerere, after a relatively peaceful (compared with neighbouring Kenya, for instance) transition to independence. One-party rule ended in 1995 with the first democratic elections held. Today the President is Jakaya Mrisho Kikwete, elected in 2005.

Tanzania's location at the crossroads of southern, central and eastern Africa leaves it vulnerable to activities, such as smuggling and the trafficking of narcotics, arms, and humans, that generate illicit revenue. The major profit generating crimes in Tanzania include theft, robbery, corruption, smuggling of precious metals and stones,

and drug trafficking, with money laundering more likely to occur in the informal non-bank sectors. Mobile banking services, such as Mpesa and AirtelMoney, are growing rapidly in Tanzania, opening up formerly underserved rural areas to formal banking, but also creating new vulnerabilities in the financial sector. Criminals have been known to use front companies, hawaladars and bureaux de change to launder funds. Real estate and used car businesses also appear to be sources of money laundering. The use of front companies to launder money appears to be more common on the island of Zanzibar. Officials indicate money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry. Bulk cash smuggling is also a problem. Tanzania is a source, transit, and destination country for men, women, and children subjected to forced labour and sex trafficking; the exploitation of young girls in domestic servitude continues to be Tanzania's largest human trafficking problem.

The Financial Action Task Force (FATF) included Tanzania in its October 19, 2012 Public Statement for its failure to adequately implement its action plan to address noted anti-money laundering/counter-terrorist financing (AML/CFT) deficiencies. Tanzania needs to implement procedures for identifying and freezing terrorist assets.

Madagascar

Formerly an independent kingdom, Madagascar became a French colony in 1896 but regained independence in 1960 and following lengthy one party rule free elections were held in 1992-93. Whilst alternating governments held power, the military intervened in 2009 in a coup following protests which toppled President Ravalomanana and installed as President the mayor of Antananarivo, Andry Rajoelina. Numerous attempts have been made by regional and international organisations to resolve the subsequent political gridlock by forming a power-sharing government and attempts are being made to hold new elections, likely to be contested by President Rajoelino and by his predecessors wife.

Madagascar is a producer and consumer of domestic cannabis and a transshipment point for heroin.

Madagascar's 3,000 miles of coastline facilitates smuggling and money laundering. Criminal proceeds laundered in Madagascar derive mostly from domestic criminal activity, but are often linked to international trade. The major sources of money laundering proceeds are tax evasion and customs fraud. Illegal mining activities and mineral resources including gemstones smuggling, protected flora and fauna smuggling, illegal logging, public corruption, and foreign currency smuggling are also areas of concern.

Central Africa



Central Africa is a core region of the African continent which includes Burundi, the Central African Republic, the Democratic Republic of the Congo, and Rwanda, but could also include a larger number of countries including also: Angola, Cameroon, Chad, the Republic of the

Congo, Equatorial Guinea, Gabon, and São Tomé and Príncipe. All these countries are members of the Economic Community of Central African States (ECCAS).

Central Africa is a region that is primarily inhabited by Bantu peoples originally from present-day Nigeria. Bantu languages predominate, with Chadic and Nilo-Saharan languages also spoken in some areas. Christianity, mixed with traditional beliefs in some places, is the predominant religion in Central Africa.

Central Africa is also home to the most terrible genocide of the late twentieth century, which took place in Rwanda in 1994, which played a part in and led to the Congo Wars in 1996 and 1998 (also known as the Great War of Africa) which officially ended in July 2003. The Great War of Africa was the deadliest war in modern African history, directly involving nine African nations, as well as about 20 armed groups. By 2008, the war and its aftermath had killed 5.4 million people, mostly from disease and starvation.

Rwanda

Rwanda's history is dominated by the events that took place in 1994 and their aftermath which continue to shape the future of the region. A coup in 1973, installed a President from the majority Hutu people and with the imposition of one party rule, the minority Tutsis were subject to serial abuse and many fled to neighboring countries including Uganda, where under the umbrella of the Rwandan Patriotic Front (RPF), the Tutsis fought back, unsuccessfully invading Rwanda in 1989, and again in 1990 with a Civil war the result. In 1993 the civil war ended with a peace accord granting increased rights to Tutsis at the cost of almost 1 million lives lost. With a shaky peace still in place, the Hutu Rwandan President Juvénal Habyarimana returned by plane from a regional summit in Tanzania, a surface-to-air missile hit his plane killing all on board over Rwanda's capital city of Kigali. Hutu extremists reacted angrily, taking over the government, they blamed the Tutsis for the assassination and began a slaughter that would be later called a genocide. Lasting 100 days, the Rwanda

genocide left approximately 800,000 Tutsi and Hutu sympathisers dead. The genocide was carried out by the Army for the Liberation of Rwanda, which was formed by the amalgamation of FAR (the armed forces of the Rwandan Hutu regime) and the civilian militia forces known as the Interhamwe. The Rwanda Genocide ended only when the RPF finally responded and took over the country.

Following the RPF's success, over a million Hutus, including most of those implicated in the genocide, fled to Zaire (now the Democratic Republic of the Congo), setting up camps of refugees in Eastern Congo near Goma and re-establishing the Interhamwe who began to work with the then Congolese government and agitating and destabilising the region. Rwandan forces, with support from Uganda, allied with the Congolese opposition led by Laurent Kabila, attacked in 1996, dispersing the Goma camps, and forcing the majority of Hutu exiles to return to Rwanda, while pushing the Interhamwe deeper into Congo and further from the Rwandan border.

Rwanda is led by President Paul Kagame, in office since 2000 and elected to a second 7 year term in 2010.

The Rwandan financial system remains relatively unsophisticated, although the number of electronic fund transfers and credit card transactions is rising. Money transfers by cell phone are becoming common. While the black market for smuggled goods is limited, the smuggling of tin, tantalum, tungsten, and gold from neighboring Democratic Republic of Congo generates funds which may be laundered through Rwanda's financial system. The scope of this smuggling is difficult to quantify.

Army for the Liberation of Rwanda (ALIR) (Hutu) - Rwanda / DRC

The Army for the Liberation of Rwanda (ALIR) was formed in 1994 from the amalgamation of FAR (the armed forces of the Rwandan Hutu regime) and the civilian militia force known as Interahamwe. These two groups were responsible for the genocide carried out against the Tutsi community in 1994 in which more than 500,000 men, women and children lost their lives. Many moderate Hutus also fell victim to this genocidal rampage. The merger of the two groups occurred as they were forced out of Rwanda into the Democratic Republic of Congo by the shift in power from the majority Hutu ethnic community to that of the Tutsis. Formulated with the objective of restoring Hutu control in Rwanda, the ALIR functions as the armed wing of the Party for the Liberation of Rwanda. It is also feared that the ALIR intends to complete the genocide of the smaller Tutsi community that it began in 1994.

The activities of the ALIR have not however been restricted to the Tutsi community; members of ALIR have also targeted foreign nationals from countries

believed to support the Tutsi government. For instance in 1999 ALIR militants captured and killed 8 foreign tourists visiting a game reserve in the Congo-Ugandan border area. The attack was allegedly in response to UK and US governmental support for the Tutsi regime. The ALIR also participated in the Congo Civil War, aligning itself with the Democratic Republic of Congo's government to help quell the uprising following the Rwandan government's declaration of support for the uprising. Consequently the Democratic Republic of Congo provided the ALIR with training camps and funding in exchange for its military aid. This allowed the ALIR to conduct operations in Rwanda alongside its Congolese campaign.

In 2001 the ALIR was replaced by the Democratic Front for the Liberation of Rwanda (FLDR), a group that has established links with other insurgent groups in Rwanda and continues to operate near the Rwandan border in the east of the Democratic Republic of Congo. In 2002, following the withdrawal of Rwandan troops from eastern Congo, the Democratic Republic of Congo ceased its financial support for the FLDR. The FLDR is believed still active.

Rwandan Patriotic Army (Tutsi) - Rwanda

The Rwandan Patriotic Army (RPA) is the military wing of the Tutsi political movement known as the Rwandan Patriotic Front (RPF). The group was founded in 1985 in Uganda and composed of exiled Rwandan Tutsis who had fled their homeland in order to escape the violence directed at their community by the Hutu ethnic tribe. In 1989 the RPA invaded Rwanda in an attempt to seize back power from the Hutu government, however the campaign was unsuccessful and the RPA retreated to Uganda.

In 1990 the RPA, having regrouped, renewed the invasion and crossed into Rwanda with approximately 10,000 soldiers under the command of Major General Rwigyema. With this move began a conflict that endured for three years, descending into a campaign based largely on guerrilla insurgency and widely held to have cost the lives of 800,000 people. In 1993 the Civil War ended with the signing of a power sharing agreement, however by 1994 the peace had been broken and the interim government initiated a campaign against Tutsis and moderate Hutus that has become known as the 1994 Rwandan Genocide. In response to this assault the RPA restarted its violent campaign against the Rwandan government and by July of 1994 had taken control of the entire country. Having seized power through the military efforts of the RPA the RPF swore in a transitional government. However this development did not spell the end of ethnic violence in Rwanda, with the RPA (now known as the Rwandan Defence Forces) exacting devastating retribution against the Hutu community. According to Amnesty International up to 200,000 lives were claimed in this ethnic violence.

Democratic Republic of the Congo

A former Belgian colony, known in 1907 as the Belgian Congo, independence was achieved in 1960, and it was renamed the Democratic Republic of the Congo. In 1965 a coup would install military leader Mobutu Sese Seko who renamed the country the Republic of Zaire ruling the country for more than 30 years, a rule noted for its brutality and corruption. With the end of the cold war a weak Mobutu government was being affected by events in neighbouring Rwanda. By 1996, the war and genocide in neighbouring Rwanda (see above) had spilled over to Zaire. Rwandan Hutu militia forces (Interahamwe), who fled Rwanda following the ascension of a Tutsi-led government, were using Hutu refugee camps in eastern Zaire as bases for incursions against Rwanda. Rwandan troops, Rwandan Patriotic Front (RPA) entered Zaire, and allied with Ugandan forces and the local armed opposition led by Laurent-Desire Kabila known as the Alliance of Democratic Forces for the Liberation of Congo-Zaire (AFDL), they attacked both the Interhamwe and the Mobutu regime. The Interhamwe fled deeper into the Congo and away from the Rwandan border region and the government forces were eventually defeated when in May 1997, Mobutu left the country, and Kabila became President.

This could have seen an end to the regional conflict with decisive victories both in Rwanda and Congo achieved by allies. However by 1998, the once time allies had become enemies, once Kabila ordered all foreign troops to leave the Congo. By 1999, the DRC was divided de facto into three segments, each controlled by the Congolese government, backed also by Angolan, Namibian and Zimbabwean troops and Ugandan backed troops and Rwandan backed troops with the parties controlling each segment but with a military deadlock between them. The breakthrough came in 2001 with the assassination of Laurent Kabila who whilst succeeded by his son, Joseph Kabila, who agreed to power sharing taking effect in 2003. Whilst the Country is much more stable, conflict still remains, particularly in Eastern Congo with Rwandan Tutsi supported groups such as M23 continuing.

Much of the fighting is thought to also involve control of the Congo's mineral wealth which is the mainstay of the economy. Mining is centered in Katanga province. Products include: copper, cobalt, zinc, manganese, uranium, cassiterite (tin ore), coal, gold, and silver. Diamonds are mined in Kasai. There are major deposits of petroleum offshore near the mouth of the Congo River. About 75% of the Congo is covered with forest containing ebony and teak as well as less valuable woods. Since 1994 diamonds have become the country's leading export following a decline in the production of copper (once the leading mineral product in terms of

value). The country produces much of the world's small industrial diamonds. Most economic activity in the DRC takes place in the informal sector, estimated to be up to ten times the size of the formal sector, with most transactions, even those of legitimate businesses, carried out in cash. Bribery and Corruption, customs and tax fraud, tax evasion, misappropriation of public funds, the sale of prohibited products and services, and illegal exploitation of minerals and other valuable materials are common. Casinos and smuggling of gold, diamonds, and weapons also are important sources of untracked money. Gold and diamonds are extensively mined in and routinely smuggled out of the DRC, and most of those cash transactions take place in US dollars. Due to its large geographic size, lack of a functional judicial system, and dominant informal sector, the DRC is particularly vulnerable to money laundering. The DRC is ranked 154 out of 175 in the 2013 Transparency International Corruption Perceptions Index. The DRC is subject to UN, US, and EU sanctions, including an arms embargo, and travel bans and asset freeze orders against members of militia and rebel groups. For more details see Part 1 Section 3 Money Laundering Laws and Regulations.

Republic of the Congo / Congo-Brazzaville

The original human settlers in the region were pygmies, followed in the 13th century by Bantu tribes from Nigeria and then followed by the Europeans in the 15th Century. The French dominated the region, occupying it and then making it part of French Equatorial Africa in 1910, which was established to bring together four territories: Gabon, Middle Congo (now the Republic of the Congo), Oubangui-Chari (now the Central African Republic) and Chad, with the Central authority based in Brazzaville, now the capital of the Congo. Under France's Fourth Republic (1946–58), the federation was represented in the French parliament. When the territories voted in the September 1958 referendum to become autonomous within the French Community, the federation was dissolved. In 1959 the new republics formed an interim association called the Union of Central African Republics, before becoming fully independent in August 1960. A quarter century of experimentation with Marxism was abandoned in 1990 and a democratically elected government took office in 1992. A brief civil war in 1997 restored former Marxist President Denis Sassou-Nguesso, leading to unrest until a final peace accord in 2003, though the calm is uneasy. The Republic of Congo is one of Africa's largest petroleum producers. The Republic of the Congo is not a major regional financial center nor is it a major narcotics destination or source country, although the port city of Pointe Noire is frequently utilised as a transit point for narcotics moving north to Europe. Most financial crimes involve domestic corruption and embezzlement. The ROC's

economy is heavily cash dependent, relying very little on electronic transfers and cheques. Laundering money through investment in real estate is reportedly a growing problem.

Gabon

Gabon has a similar history to the Congo above and like its former French Equatorial African brethren it gained its independence in 1960. Since that time Gabon has had two long serving president dictators. The first was Leon M'ba and the second was Omar Bongo, who would rule the country for more than 30 years until his death in 2009 ruling as a corrupt dictator for most of this period. He was succeeded by his son, Ali Bongo Ondimba. Gabon suffers from porous borders; and smuggling, which is facilitated by organised criminal groups, is widespread. Despite reform efforts, systemic corruption still exists, with embezzlement of state funds, including by politically exposed persons (PEPs), giving rise to money laundering.

Central African Republic

From the 16th to 19th century, the people of this region were ravaged by slave traders. The French occupied the region in 1894. As the colony of Ubangi-Shari, what is now the Central African Republic was united with Chad in 1905. In 1910 it was joined with Gabon and the Middle Congo to become French Equatorial Africa and gained its independence after its dissolution. After many governments of different stripes, many of whom can be considered corrupt, the country is today one of the world's poorest and unstable. Following a recent coup, Michel Djotodia has become President in 2013. The economy is almost entirely cash-based and corruption is widespread. Smuggling of contraband including diamonds and weapons is believed to occur across the unsecured border areas with Chad and Sudan, while undocumented trade across the river with the Democratic Republic of the Congo involves primarily domestic or agricultural goods.

Chad

Chad, part of French Equatorial Africa until 1960, it has since endured three decades of civil warfare, as well as invasions by Libya, before peace was finally restored in 1990. The government eventually drafted a democratic constitution and held flawed presidential elections in 1996 and 2001. In 1998, a rebellion broke out in northern Chad, which has sporadically flared up despite several peace agreements between the government and the insurgents. In 2005, new rebel groups emerged in western Sudan and made probing attacks into eastern Chad despite signing peace agreements in 2006 and 2007. President Idriss Deby was reelected again in 2011

to his fourth term, with power in the hands of an ethnic minority. Contraband and smuggling vary by region in Chad. Along the southern and western borders, the contraband goods market consists largely of foodstuffs, cigarettes, fuel, and household items smuggled to avoid import duties. Across Chad's northern desert, which is sparsely populated and transected by Sahelian trade routes, smuggled items include drugs and weapons. Some of these items transit Chad rather than remain in the domestic market. Chad is rated 163 out of 175 in the 2013 Transparency International Corruption Perceptions Index.

Burundi

Burundi is a landlocked country in the Great Lakes region of Eastern Africa, bordered by Rwanda to the north, Tanzania to the east and south and the Democratic Republic of the Congo to the west. Burundi is one of the five poorest countries in the world. The Twa, Hutu and Tutsi peoples have lived in Burundi for at least five hundred years and, for over two hundred years, Burundi was ruled as a kingdom. Burundi's first democratically elected president was assassinated in October 1993 after only 100 days in office, triggering widespread ethnic violence between Hutu and Tutsi factions. More than 200,000 Burundians perished during the conflict that spanned almost a dozen years. In 2005, and elected a majority Hutu government in 2005. The government of President Pierre Nkurunziza who was re-elected in 2010, continues to face many political and economic challenges, with corruption endemic, according to Transparency International, Burundi is ranked 157 out of 175 in its 2013 Corruption Perceptions Index.

Cameroon

French Cameroon became independent in 1960 as the Republic of Cameroon. The following year the southern portion of neighboring British Cameroon agreed to merge to form what is Cameroon today. The country has been one of the more stable in the region, albeit with slow movement toward democratic reform. Power remains firmly in the hands of President Paul Biya. Instability in neighbouring countries and the use of a common currency have resulted in Cameroon being used as a conduit to move funds from those countries to Europe. Terrorist activity in neighbouring countries, illicit wildlife trafficking and maritime piracy present vulnerabilities and their proceeds may facilitate the movement and activities of terrorists and drug trafficking organisations. Its economy is heavily cash dependent. Trade-based money laundering is rampant. Cameroon is particularly vulnerable to the abuse of cross-border bulk currency movements and exploitation by companies transferring money internationally. Most foreign currency transactions are in euros or dollars.

São Tomé and Príncipe

São Tomé and Príncipe consists of two archipelagos around the two main islands: São Tomé and Príncipe, off the northwestern coast of Gabon, being islands that are part of an extinct volcanic mountain range. São Tomé, the sizable southern island, is situated just north of the equator. With an estimated population of 172,000, São Tomé and Príncipe is the second-smallest African country (Seychelles is the smallest African country). Originally claimed by Portugal in the late 15th century, independence was only achieved in 1975. A new government of Prime Minister Gabriel Arcanjo Ferreira Da Costa took office in 2012. The recent discovery of oil in the Gulf of Guinea promises to attract increased attention to the small island nation.

Equatorial Guinea

A former Spanish colony, Equatorial Guinea is a small country in West Africa which gained its independence in 1968. It is today sub-Saharan Africa's third biggest oil producer. Current President Teodoro Obiang Nguema Mbاسogo, came to power in a coup in 1979, following the reign of terror if his predecessor Francisco Macias Nguema.

According to Human Rights Watch, the "dictatorship under President Obiang has used an oil boom to entrench and enrich itself further at the expense of the country's people". Transparency International has put Equatorial Guinea in the top 12 of its list of most corrupt states raking it 163 out of 176. Resisting calls for more transparency, President Obiang has for long held that oil revenues are a state secret. A 2004 US Senate investigation into the activities of US Bank, Riggs Bank found that President Obiang's family had received huge payments from US oil companies including from Exxon Mobil. Global Witness has been lobbying governments to act in particular against the President and his son, Teodoro Obiang, on corruption grounds, though as Obiang's son is a government minister, both enjoy some sovereign immunity protections. For more details see Part 2 Section 7 below. Equatorial Guinea also hit the headlines in 2004 when the start of an attempted coup was intercepted in Zimbabwe just before they were about to depart to overthrow President Obiang. For more details see Part 2 Section 7 Simon Mann below. Beyond concerns over corruption, human trafficking concerns are the most serious. Equatorial Guinea is a source and destination country for women and children subjected to forced labour and sexual exploitation. Women and children have been trafficked from Cameroon, Benin and other neighboring countries for work as domestic servants, and to for forced labour or prostitution; Equatorial Guinean girls may be encouraged by their parents to engage in the sex trade in urban centers to receive groceries, gifts, housing, and money.

Southern Africa



Southern Africa comprises Botswana, Lesotho, Mozambique, Namibia, South Africa, Swaziland, Zambia, and Zimbabwe. The region shares many of the same experiences of other regions in sub-Saharan Africa, with settlements of Bantu-speaking peoples moving south of the Limpopo River by the 4th or 5th century BC. They also shared similar colonial experiences, with European colonial rule being firmly established in the Nineteenth Century during the so called scramble for Africa. However whilst much of Africa gained independence in the 1960s, Independence took much longer in Southern Africa, where European settler colonies tended to be more entrenched and lasted longer than in the rest of Africa. European settler colonies existed in South Africa, Zimbabwe, Namibia, Angola, and Mozambique, and consequently, these African countries were among the last to achieve independence. For example Angola and Mozambique in the 1970s; Zimbabwe in 1980; and Namibia in 1990.

South Africa became a minority-led republic in 1961 and achieved majority-rule in 1994). In many cases, the end of white minority rule required armed struggle on the part of Africans in order to achieve independence.

After independence, the countries that fought wars of independence implemented largely socialist or redistributionist policies, which made them targets of external interference and destabilization. Angola and Mozambique experienced punishing retribution from South Africa and the US for turning to the Eastern bloc for support. Moreover, whether a country committed itself to socialist policies or not, they all found themselves confronting the South African apartheid state, which was determined to maintain economic and military authority in the region at any cost. Finally, the countries of the region have a long history of economic interdependence.

Because of South Africa's dominance, neighboring countries were dependent upon South Africa for trade, transportation (especially the land-locked countries), and communication. In addition, migrants from neighboring Botswana, Mozambique, Swaziland, and Lesotho historically journeyed to South Africa to work in that country's agricultural, mining, and manufacturing industries. The earnings that migrants made became crucial to the survival of families left back home. Eventually, Southern African countries created regional integration schemes, among them the Southern African Customs Union and the Southern African Development Community, to improve their economic fortunes and develop cooperative security regimes.

South Africa

Dutch traders landed at the southern tip of modern day South Africa in 1652 and established a stopover point on the spice route between the Netherlands and the Far East, founding the city of Cape Town. After the British seized the Cape of Good Hope area in 1806, many of the Dutch settlers (the Boers) trekked north to found their own republics. The discovery of diamonds (1867) and gold (1886) spurred wealth and immigration and intensified the subjugation of the native inhabitants. The Boers resisted British encroachments but were defeated in the Boer War (1899-1902); however, the British and the Afrikaners, as the Boers became known, ruled together beginning in 1910 under the Union of South Africa, which became a republic in 1961 after a whites-only referendum. In 1948, the National Party was voted into power and instituted a policy of apartheid, the separate development of the races, which favoured the white minority at the expense of the black majority.

The African National Congress (ANC) led the opposition to apartheid and many top ANC leaders, such as Nelson Mandela, who recently passed away and who spent decades in South Africa's prisons. Internal protests and insurgency, as well as boycotts by some Western nations and institutions, led to the regime's eventual willingness to negotiate a peaceful transition to majority rule. The first multi-racial elections in 1994 brought an end to apartheid and ushered in majority rule under an ANC-led government, under President Mandela. Current President and ANC leader is Jacob Zuma, who won general elections in 2009.

South Africa, as its name suggests is located at the southern tip of Africa and is the 25th-largest country in the world by land area, and with close to 53 million people, it is the world's 24th-most populous nation. South Africa is a multiethnic society encompassing a wide variety of cultures, languages, and religions, including Europeans and Asians but still dominated with 80% of black African ancestry.

Its economy is the largest and most developed in Africa and the 28th-largest in the world, although poverty and inequality remain widespread, with about a quarter of the population unemployed and living on less than US\$1.25 a day. South Africa though is plagued by serious corruption concerns with Transparency International ranking the country 69 out of 176 in its 2012 Corruption Perceptions Index and a high crime rate. A survey for the period 1998–2000 compiled by the UN Office on Drugs and Crime ranked South Africa second for assault and murder (by all means) per capita and first for rapes per capita in a data set of 60 countries. Total crime per capita ranked South Africa as 10th overall. Whilst around 50 people are murdered in South Africa each day, the murder rate has reduced by 50%. In the period 1994 to 2009. The annual crime statistics

released in 2011 show a continuing downward trend, except for rape, which went up by 2.1%.

The country has one of the highest rates of rape in the world, with some 65,000 rapes and other sexual assaults reported for the year ending in March 2012, or 127.6 per 100,000 people in the country. The incidence of rape has led to the country being referred to as the "rape capital of the world". South Africa has amongst the highest incidences of child and baby rape in the world. If the rapist is convicted, his prison time would be around 2 years.

South Africa also has a high record of car hijackings when compared with other industrialised countries. Certain high-risk areas are marked with road signs indicating a high incidence of car hijackings within the locality. Crime against commercial white farmers is also particularly high, and the issue continues to attract significant media attention. As far as white collar fraud is concerned, according to PricewaterhouseCoopers' fourth biennial Global Economic Crime Survey in 2005, 83% of South African companies reported being affected by white collar crime in 2005, whilst 72% of South African companies reported being affected in 2007.

South Africa's position as the major financial center in the region, its sophisticated banking and financial sector, and its large, cash-based market make it vulnerable to exploitation by transnational and domestic crime syndicates. The largest source of laundered funds in the country is proceeds from the narcotics trade. Fraud (advance fee scams, beneficiary maintenance fraud, and deposit refund scams), theft, racketeering, corruption, currency speculation, credit card skimming, poaching, theft of precious metals and minerals, human trafficking, stolen cars, and smuggling of goods are also sources of laundered funds. Many criminal organisations also are involved in legitimate business operations.

In addition to criminal activity by South African nationals, observers note criminal activity by Nigerian, Pakistani, Andean, and Indian drug traffickers; Chinese triads; Taiwanese groups; Bulgarian credit card skimmers; Lebanese trading syndicates; and the Russian mafia. Investment clubs, known as stokvels, have been used as cover for pyramid schemes. In some instances, nominee structures have been exploited by criminals who intend to launder illicit funds by mixing them with legitimate assets held on someone else's behalf. There is a significant black market for smuggled and stolen goods. South Africa is a transshipment center for heroin, hashish, and cocaine, as well as a major cultivator of marijuana. It is also the world's largest market for illicit methaqualone, usually imported illegally from India through various east African countries, but increasingly producing its own synthetic drugs for domestic consumption. South Africa is also home to a number of domestic organised criminal gangs, including the [People Against Gangsterism and Drugs](#) and the [Numbers Gang](#).

People Against Gangsterism and Drugs - South Africa

People Against Gangsterism and Drugs (PAGAD) was a muslim vigilante group formed in 1996 in the Cape Flats area of Cape Town, South Africa, emanating out of Qibla a small South African Islamic extremist group led by Achmad Cassiem, who was inspired by Iran's Ayatollah Khomeini. Cassiem founded Qibla in the 1980s, seeking to establish an Islamic state in South Africa. PAGAD began in 1996 as a community anticrime group fighting drug lords in Cape Town's Cape Flats section.

PAGAD now shares Qibla's anti-Western stance as well as some members and leadership. Though each group is distinct, the media often treat them as one. Both use front names including Muslims Against Global Oppression (MAGO) and Muslims Against Illegitimate Leaders (MAIL) when launching anti-Western campaigns.

PAGAD was originally initiated by a handful of muslim neighbourhood watch members from a few Cape Town townships who decided to organise public demonstrations to pressure the government to fight the illegal drug trade and gangsterism that was affecting their communities. However, PAGAD increasingly took matters into their own hands, believing the police were not taking enough action against gangs. Initially the community and police were hesitant to act against PAGAD activities, recognising the need for community action against crime in the gang-ridden communities of the Cape Flats. Notorious gangsters were initially asked by PAGAD members to stop their criminal activities or be subject to 'popular justice'. For those that refused or ignored warnings, PAGAD members would set fire to drug dealers houses and kill gangsters. PAGAD's campaign came to prominence in 1996 when a local gang leader was beaten and burnt to death by a mob during a march to his home. South Africa's police quickly came to regard PAGAD as part of the problem, rather than a partner in the fight against crime and they were eventually designated a terrorist organisation by the South African government.

The threat of growing vigilantism in 2000 led the Western Cape provincial government to declare a 'war on gangs' that became a key priority of the ANC government at the time. Although PAGAD's leadership denied involvement, they were believed to be responsible for killing a large number of gang leaders, and also for a bout of urban terrorism particularly bombings in Cape Town, targeting gang leaders, bombing targets including South African authorities, moderate Muslims, synagogues, gay nightclubs, tourist attractions, and Western-associated restaurants, including in 1998 the Cape Town Planet Hollywood, leaving 2 dead and 26 injured allegedly in response to US strikes against Sudan. Today, PAGAD maintains a small and less visible presence in the Cape Town Muslim community.

Numbers Gang - South Africa

The Numbers Gang is an umbrella term encompassing South Africa's three most prominent prison gangs, 28s, 27s and 26s. The origin of these groups can be traced back to the late nineteenth century when sects were established amongst working men residing in all male compounds at Witwatersrand mine near Johannesburg. These gangs were therefore originally formed outside prisons, however during the apartheid system, when imprisonment became a commonplace experience for black South Africans who failed to carry their identification passes, prisons soon became a convenient meeting place and organisational hub. As a result the Numbers gang is now firmly entrenched within South African Prisons.

The organisational structure of the Numbers gang is relatively sophisticated, emulating that of military institutions in its strict hierarchical order. Rigid discipline is also enforced in similar military fashion, and much like the armed forces ranks are transferable, both between prisons and between the internal world of the prison and the external free community. Members are even punished for transgressions by an internal tribunal process. The distinct subsections within the numbers gang, known as 28s, 27s and 26s, perform specific roles within the organisation. Members of the 28s are regarded as the most senior echelon of the group, providing its leadership and allowing themselves to possess 'wifes' (a jail term for a male partner). 27s is responsible for the enforcement of rulings made by the other two groups, while the final third of the tripartite system, 26s, is assigned the task of yielding revenue for the group. Members of this rank specialise in fraud, theft and the trade of illegal substances.

Angola

Angola achieved its independence from Portugal in 1975, but then suffered a 27-year civil war which only ended in 2002. Fighting between the Popular Movement for the Liberation of Angola (MPLA), led by Jose Eduardo Dos Santos, who led the government and the National Union for the Total Independence of Angola (UNITA), led by Jonas Savimbi, cost up to 1.5 million lives, with another 4 million people displaced. Savimbi's death in 2002 ended UNITA's insurgency and cemented the MPLA's hold on power. President Dos Santos was re-elected as President once again in 2012.

Whilst Angola does not produce large quantities of drugs it is nevertheless a transit point for drug trafficking, particularly for drugs brought in from Brazil and South America destined for Europe. Increasingly, Angola is becoming a destination point as well with a growing market for illicit drugs. Angola's borders are porous and vulnerable to general smuggling and trafficking in small arms, diamonds, humans, and motor vehicles. Angola has a high rate of U.S. dollar cash flow.

The laundering of funds derived from widespread corruption is also a concern. Corruption remains a serious problem in Angola with according to Transparency International, Angola ranking 153 out of 175 countries in its 2013 Corruptions Perceptions Index.

National Union for the Total Independence of Angola (UNITA) - Angola

The National Union for the Total Independence of Angola (UNITA) was a rebel group originally formed in 1966 to fight for Angolan independence from Portugal. However following the rise to power in 1975 of the Movimento de Libertao de Angola (MPLA) in place of the Portuguese, UNITA's allegiances were drastically reversed; the group accepted the financial support of Portugal and other Western nations in order to violently oppose the new government of Angola. A great deal of this Western support was derived from anti-Soviet sentiment and the identification of the new Marxist-Leninist Angolan government as a proxy of the Soviet state. The conflict between the MPLA and UNITA soon progressed into the Angolan Civil War, a struggle perceived as highly significant in the geopolitical balance of power during the Cold War. Though broken up by short periods of peace, the conflict endured for 27 years and is reported to have claimed somewhere in the region of 500,000 lives.

During this bloody war UNITA perpetrated attacks against civilians that appeared to demonstrate little more than wanton violence and led to the group's characterization as a terrorist group. For instance in 2001 UNITA reportedly bombed the Angolan civilian railway, resulting in the deaths of more than 150 civilians.⁸ In 2002 UNITA forces admitted defeat and the Civil War came to an end. Since then UNITA has participated peacefully in the electoral process, standing in the 2008 elections and winning 16 seats. However UNITA represents a fitting reminder of the dangers inherent in attempting to influence the domestic politics of a nation in the interests of international politics. A poignant commentary on the use of such politically motivated foreign aid in local conflicts is provided by Guardian journalist Victoria Brittain, who, speaking of UNITA's leader Jonas Savimbi notes that "The CIA embraced Savimbi as warmly, and as unthinkingly, as it did bin Laden. Both were dependable anti-communists. Both became terrorists."

Lesotho

Formerly Basutoland, the country was renamed the Kingdom of Lesotho on its independence from the UK in 1966. In 1998, violent protests and a military mutiny following a contentious election prompted a brief but bloody intervention by South African and Botswana military forces. After continued instability, finally elections in 2012 produced a representative coalition government under Prime Minister Motsoahae Thomas Thabane.

While there is not a significant black market for smuggled goods in the country, undeclared and undeclared items pass between Lesotho and South Africa daily. The vast majority of smuggling is low level and committed by individuals. Smugglers commonly bring undeclared consumer goods or occasionally larger items like automobiles from South Africa into Lesotho. There is some evidence of more illicit activity as small arms are smuggled across Lesotho's porous border, often in exchange for Lesotho-grown marijuana.

Namibia

Namibia, formerly the German colony of South-West Africa, was annexed by South Africa after World War II. In 1966 the Marxist South-West Africa People's Organisation (SWAPO) guerrilla group launched a war of independence for the area that became Namibia, but it was not until 1988 that South Africa agreed to end its interest and usher in Namibian independence in 1990. When Namibia gained its independence SWAPO became the dominant political party, with its head, Sam Nujoma, elected as Namibia's first President. Nujoma had the constitution changed so he could run for a third term in 1999, but in 2004 he was replaced as the SWAPO presidential candidate by Hifikepunye Pohamba, who has been described as Nujoma's hand-picked successor. SWAPO continues to dominate Namibian politics, continuing still as the governing party winning 75.25% of the popular vote and 54 out of 72 seats in the parliamentary election held in November 2009.

Sources of money laundering in Namibia are related to both regional and domestic criminal activities. Falsification or misuse of identity documents, customs violations, trafficking of precious metals and gems, trafficking in illegal drugs, and stolen vehicles - mostly from South Africa, are regional problems that affect Namibia. Organised crime groups involved in smuggling activities generally use Namibia as a transit point, particularly for goods destined for Angola. Domestically, real estate as well as minerals and gems are suspected of being used as vehicles for money laundering. Namibian authorities believe the proceeds of these activities are laundered through Namibian financial institutions, but on a small scale. The organised fencing of stolen goods, not just vehicles, is also a problem in Namibia. Namibia is predominantly a country of origin and destination for children and, to a lesser extent, women subjected to forced labour and sex trafficking.

Mozambique

Almost five centuries as a Portuguese colony came to a close with independence in 1975. Large-scale emigration, economic dependence on South Africa, a severe drought and a prolonged civil war hindered the country's development until mid-1990s. The ruling Front for the Liberation of Mozambique (Frelimo) party formally

abandoned Marxism in 1989, and a new constitution the following year provided for multiparty elections and a free market economy. A UN-negotiated peace agreement between Frelimo and rebel Mozambique National Resistance Movement (Renamo) forces ended the fighting in 1992. In December 2004, Mozambique underwent a delicate transition as Joaquim Chissano stepped down after 18 years in office. His elected successor, Armando Emilio Fuebuza, was reelected to a second term in October 2009. However, the elections were flawed by voter fraud, questionable disqualification of candidates, and Frelimo use of government resources during the campaign. As a result, Freedom House removed Mozambique from its list of electoral democracies.

Mozambique is a transit point for South Asian hashish and heroin, and South American cocaine probably destined for the European and South African markets. Money laundering is linked principally to customs fraud and drug trafficking. Local organised criminal groups control narcotics trafficking operations in the country and are thought to involve networks with links to Pakistani and Indian nationals and immigrants. Authorities believe the proceeds from these illicit activities have helped finance commercial real estate developments, particularly in the capital. While money laundering in the banking sector is considered to be a serious problem, foreign currency exchange houses, cash couriers, and the hawala remittance system play more significant roles in financial crimes and money laundering. Black markets for smuggled goods and informal financial services are widespread, dwarfing the formal retail and banking sectors in most parts of the country. The laundering of funds derived from widespread corruption is also a concern. Corruption remains a serious concern in Mozambique with, according to Transparency International in 2013 Mozambique ranking 119 out of 175 in its 2013 Corruptions Perception Index.

Mozambique National Resistance Movement (RENAMO) - Mozambique

The Mozambican National Resistance (Resistencia Nacional Mocambicana -- Renamo) was formed in 1976 in response to the ascension to power of the Communist group known as the Front for the Liberation of Mozambique (Frelimo) in 1975. The foundation of the Renamo was in large part orchestrated by Rhodesia's white minority government, which feared that Frelimo would encourage resistance to white rule in Rhodesia and may go so far as to provide support for rebels attempting to seize power. To pre-empt any possible disruption to their status-quo, the Rhodesian government founded Renamo to actively combat Frelimo forces based in Mozambique. The organisation was made up of a range of groups opposed to the new Frelimo government; disillusioned former Frelimo members, opponents of the Marxist-Leninist Frelimo government, and soldiers of the former Portuguese colonial army all joined forces to combat the new rulers of Mozambique.

This armed resistance posed by Renamo to the new

government of Mozambique resulted in the initiation of the Mozambican Civil War in 1977, a conflict estimated to have cost around 1 million lives and whose legacy is still felt today with undetonated landmines continuing to cause casualties. In 1980, with the collapse of minority white rule in Rhodesia and the emergence of Zimbabwe in its place, the funding of Renamo was taken up by South Africa as the last bastion of white rule in Africa. As part of its plan to maintain a system of Apartheid the South African government set about a policy of destabilizing its bordering African nations, consequently directing Renamo operations towards the destruction of trade and communications infrastructure in both Mozambique and the newly formed Zimbabwe. This South African sponsorship came to an end however following an accord between the governments of South Africa and Mozambique. In this 1984 concord it was agreed that Mozambique would cease its support for the ANC in South Africa, in return for the retraction of South African support for Renamo operations in Mozambique. Consequently the level of state support on which Renamo could rely was greatly reduced.

Nonetheless Renamo operations continued throughout the 1980s, until the Mozambique Civil War finally drew to a close in 1992. On 4 October 1992 the opposing Frelimo and Renamo forces signed an official peace agreement, after which Renamo began its integration back into Mozambique society and politics. Many of the Renamo forces were also assimilated into the Mozambique armed forces and by 1994 Renamo had stood as a political party in democratic elections. Renamo, while never officially designated a terrorist group, is no longer considered to be a militant group. Indeed today Renamo is Mozambique's largest opposition party, receiving 29.7% of the popular vote in the 2004 general elections, though tensions remain with Frelimo dominating the country.

Botswana

Formerly the British protectorate of Bechuanaland, Botswana adopted its new name upon gaining independence in 1966. More than four decades of uninterrupted civilian leadership, progressive social policies, and significant capital investment have created one of the most stable economies in Africa. Mineral extraction, principally diamond mining, with Botswana becoming the world's largest diamond producer dominates economic activity. The stringent institutional framework for the mining and processing of diamonds affords little opportunity for organised diamond smuggling.

Smuggling that may occur is not believed to be linked to terrorist finance or the laundering of criminal proceeds. Botswana enjoys a low level of corruption compared to other African states. Botswana though is a cash-based society and the presence of organised criminal groups is growing.

There has been an increase in the amount and frequency of major fraud committed against large organisations, e.g., banks or government departments, typically with the collusion of an employee. Botswana has established an International Financial Service Center which authorizes entities to provide financial services, covering funds management, banking services, international insurance and financial intermediary services.

Swaziland

Autonomy for the Swazis of southern Africa was guaranteed by the British in the late 19th century. Independence was granted in 1968. Student and labour unrest during the 1990s pressured King Mswati III, Africa's last absolute monarch, to grudgingly allow political reform and greater democracy, although he has backslid on these promises in recent years.

There is a significant black market for smuggled goods such as cigarettes, liquor, pirated radio cassettes, videocassettes, and DVDs transited among Mozambique, South Africa and Swaziland. There is a general belief that trade-based money laundering exists in Swaziland. Proceeds generated through corruption are a major concern, as is human trafficking. Swazi officials believe the Kingdom to be at little risk of terrorist financing.

Zimbabwe

The UK annexed Southern Rhodesia from the [British] South Africa Company in 1923. A 1961 constitution was formulated that favored whites in power. In 1965 the government unilaterally declared its independence, but the UK did not recognise the act and demanded more complete voting rights for the black African majority in the country (then called Rhodesia). UN sanctions and a guerrilla uprising finally led to free elections in 1979 and independence (as Zimbabwe) in 1980. Robert Mugabe, the nation's first prime minister, has been the country's only ruler (as president since 1987) and has dominated the country's political system since independence. His chaotic land redistribution campaign, which began in 2000, caused an exodus of white farmers, crippled the economy, and ushered in widespread shortages of basic commodities. Ignoring international condemnation, Mugabe rigged the 2002 presidential election to ensure his reelection and he remains in power after being re elected again in 2013.

Zimbabwe is a state that has undergone traumatic economic and social transition since the 1980s providing opportunities for organised criminal groups; senior state bureaucrats and entrepreneurs from the private sector, to exploit weaknesses and opportunities.

Prior to the July 2013 elections in Zimbabwe, Global Witness, a pressure group that campaigns against the corruption so often involved in the exploitation of a

country's natural resources, asked the South African Development Community (SADC) to fully investigate claims that Robert Mugabe's ZANU PF party was attempting to rig the country's elections. They said there was strong evidence that ZANU PF had acquired large amounts of money from the country's diamond mines suggesting that the electoral roll had been 'doctored'. The opposition group Movement for Democratic Change (MDC) said it has serious concerns that diamond money was now a source of "off-budget revenue for ZANU-PF. Other observers have noted that the Zimbabwe secret police (CIO) has received a donation of US\$100mio from Sam Pa, a Hong Kong based businessman, in exchange for diamonds and access to other business opportunities.

In another case reported in the 'Zimbabwe Independent' the Registrar General of Zimbabwe refused to explain why his department had paid over US\$10mio to an Israeli security firm, Nikuv International, which dealt with voter rolls and election counting. According to the newspaper the recent elections were widely seen as a "made in Israel landslide". Diamonds came up again and again and help to illustrate the current phenomena of a country which has seen since its independence, economic collapse, hyperinflation and the outward migration of millions of its brightest and best. By any criteria Zimbabwe is an authoritarian state, functioning primarily, on tribal cronyism.

Organised Crime in the sense of the presence of transnational gangs has not been detected but there are organised criminal networks which have succeeded in establishing a common criminal market for illicit goods that covers the entire Southern African sub-region. These are loose confederations not socio-ethnic –criminal groupings such as the Mafia. The main kinds of non-state organised criminal activities are armed robberies, theft of motor vehicles, extortion rackets and the smuggling of diamonds and gold. Drugs are not seen as a large problem although Zimbabwe is increasingly seen as a transhipment point into South Africa.

It is said that organised crime constitutes a serious threat to societies, because it undermines good governance and transparent economic activities, becoming closely associated with corruption and violence. In this respect crime in Zimbabwe is merely an adjunct to pre-existing corruption where the ruling elite itself can penetrate and corrupt public and private organisations with the mirror activities of organised crime penetrating into both the formal business sector and government structures.

According to Transparency International in 2013 the country is amongst those most corrupt with a score of 157 out of 175. Zimbabwe is also ranked close to last in other categories such as GDP or Health. In the case of the latter, male life expectancy at 37 years, with 34 for women. Within the public sector everyday corruption is rife but it is the corruption at the political level which embraces both public and private economic activity that

sets the tone. Indeed many commercial organisations are connected with members of the Government and the Armed Forces.

Organised crime was given a boost when the Zimbabwean government intervened in the conflict in the Democratic Republic of Congo creating opportunities to exploit the resources of that country. Joint venture partnerships, involving participation of state functionaries in private enterprise and often involving partners with strong foreign links are not uncommon in Zimbabwe as is the use of state bureaucrats to protect them from competitive tender processes. The ZANU-PF also retains control of the country's enormously valuable natural resources. The South African, Chinese, and Russian state-owned or government-linked corporations have obtained valuable mineral concessions in platinum, diamonds, gold, chrome, and nickel. Some of the profits from those mining operations are channelled to the ZANU-PF, which uses the money to buy the loyalty of the police and military. In 2011 Robert Mugabe threatened to quit the Kimberley Process the body that seeks to prevent diamonds from funding conflicts. In the event the Kimberley Process is now seen by many to be seriously compromised and weakened. The US, Canada, Australia, and the EU have imposed targeted financial sanctions and travel restrictions on political leaders and a limited number of companies and state-owned enterprises believed to have been complicit in human rights abuses and undermining institutions and processes in Zimbabwe. For more details see Part 1, Section 3, Sanctions and Embargoes above.

Zambia

Zambia, formerly Northern Rhodesia achieved its independence and acquired its new name in 1964. Elections in 1991 brought an end to one-party rule, but subsequent votes were marked by problems which led to the election of Levy Mwanawasa, who was succeeded by his vice president, in 2008 by Rupiah Banda and since in 2011 by Michael Sata.

The Zambia is a transhipment point for moderate amounts of meths and small amounts of heroin, and cocaine bound for southern Africa and Europe. The proceeds of drug transactions and money derived from public corruption are the major sources of laundered funds. Human trafficking is also a problem.

Banks, real estate agents, insurance companies, casinos, and law firms are the institutions most commonly used to launder money. Money launderers in Zambia have used structuring, currency exchanges, monetary instruments, gambling, under-valuing assets, and front businesses to launder their proceeds. Other means include securities, debit/credit cards, bulk cash smuggling, wire transfers, and false currency reporting. Further, criminals use their proceeds to purchase luxury goods such as vehicles and real estate.

Middle East



The history of the Middle East dates back to ancient times, and throughout its history, the Middle East has been a major centre of world affairs, being the birthplace of 3 of the World's most important religions, Judaism, Christianity, and Islam as well as scores of others including the less common Bahá'í faith, Mandaeism, Druze faith and others. The largest countries by population are Egypt, Iran, Turkey, Iraq, Saudi Arabia, Yemen and Syria.

The modern Middle East began after World War I, when the Ottoman Empire was defeated by the British Empire and their allies and so the Middle East became partitioned into a number of separate nations, initially under British and French Mandates. Other defining events in this transformation included the establishment of Israel in 1947.

During the Cold War, NATO and the US on one side, and the Soviet Union and Warsaw Pact on the other competed to influence regional allies, particularly as the region contained two thirds of the world's oil reserves.

Whilst the term the "Middle East" had been used, it wasn't until World War 2 when it became customary to refer to the area we now know as the Middle East by this term, in fact up until this time, it was customary to refer to areas centred around Turkey and the eastern shore of the Mediterranean as the "Near East", while the "Far East" centred on China, and the Middle East then meant the area in between. Once the British established their Middle East Command and based it in Cairo, the term "Middle East" gained broader usage and acceptance.

The region has suffered numerous wars and conflicts and remains a region where tensions within the region have dominated political and world affairs and unfortunately continues to do so, with terrorism ever present and religious and nationalist tensions regularly making headlines. The emergence of Israel as an Independent State in 1947 led to one of the worlds most enduring conflicts, that between Israel and the Palestinian's and by extension with at times much of the Arab World. The rise of Islamic Groups, to increasing tension between some extreme groups and more secular regimes and conflicts between the two branches of Islam, Shia and Sunni and with other religious orders, including Jewish and Christian have also formed part of the narrative surrounding the development of the Middle East and elsewhere over the last 6 decades.

Today, there is much concern over the pursuit by some of Islamic Jihad. According to some, and clearly revealed by Ayatollah Khomeini at the time of the Iranian Revolution, a proper reading of the Quran and an understanding of history led to the conclusion that Palestine is the focus of the religio-historical confrontation between the Muslims and their eternal enemies, the Jews (and Christians). The Muslims represent the forces of truth while the Jews (and Christians) embody the forces of apostasy. In the context, the Palestinian problem can be viewed as the core of a Western offensive that began with the early Crusades and then Napoleon's invasion of Egypt in 1798 and reached its climax in 1918 with the disintegration of the Ottoman Empire, which had symbolized Islamic unity. According to this view, Palestine was always the focus of Western imperialist designs and was meant to serve as a launch pad to take over other Muslim territories. Inasmuch as the Jewish presence in Palestine symbolizes Muslim inferiority in the modern age, commitment to Palestine cannot be framed in the narrow confines of Palestinian nationalism. Instead, it is an essentially Islamic issue and is the key to unlock the liberation and unification of the Islamic nation. The jihad in Palestine entails a commitment to two inter-related goals: the liberation of Palestine and pan-Islamic revival. Jihad is the only way to liberate Palestine argue terrorists, since Muslim victory and the elimination of Israel are foreordained by God's words in the Quran.

Israel/Palestine

The Holy Land changed hands many times through history, from the Canaanites to the Israelites, Babylonians, Romans, Crusaders, Arabs, Ottoman Turks, British, but the modern phase of the conflict began in the late 1800s, when the Zionism movement grew as a result of anti-Semitism in Europe, concluding that the best solution would be the mass exodus of Jews to a state they could call their own. By 1917, Jews comprised less than 10% of the population of Palestine and lived in relative peace among their Muslim neighbors. But as waves of Jews began to immigrate to Palestine from Europe, many of them desperately fleeing Nazi persecution, tensions rose. Between 1936 and 1939, Palestinians organised civil and armed resistance against British overlords and European Jews. When the uprising was crushed, Palestinians were largely stripped of their arms and leaders, and the Jewish and Palestinian populations became further isolated and alienated from each other. Zionist militias including the Irgun also engaged in terror attacks against both Palestinians and the British occupiers. With increasing violence and with Jews making up one-third of the population of Palestine, but owning only 7% of the land, the UN in 1947, in a narrow vote dominated by European nations and former colonies, voted to allocate 55% of Palestine for a Jewish state, called Israel and 45% for a Palestinian state. In 1948 the British withdrew and the Israelis declared independence, which sparked a region-wide war. Arabs vastly outnumbered Jews, but the Israeli's were better-armed, better-

funded, and better-organised. Following this war, the new state of Israel controlled 78% of historic Palestine, Jordan ruled the West Bank, and Egypt had control over the Gaza Strip. More than 750,000 Palestinians, half the native population of Palestine at the time, fled or were expelled from what became Israel.

In 1967, Israel launched a pre-emptive attack against Egypt after Egypt's President Nasser blockaded Israel's only access point to the Red Sea and amassed troops in the Sinai. Jordan and Syria were drawn into the conflict as well. At the end of the so-called Six Day War, Israel had captured and occupied the West Bank from Jordan, the Gaza Strip and Egypt's Sinai Peninsula, and the Syrian Golan Heights. The Sinai was returned to Egypt under a separate peace deal in 1979, but the Golan Heights and the Palestinian territories remain under Israeli occupation.

During this time the Palestinians were represented by numerous groups, many of which saw the [Palestine Liberation Organisation](#) under its leader Yasser Arafat, the head of Fatah at its center. Founded in 1964, the PLO was admitted to the UN with observer status in 1974, initially operating out of Jordan and Lebanon, engaging in guerrilla tactics in an attempt to regain Palestine by force of arms. It was expelled from Jordan in 1971 by King Hussein, then expelled from Lebanon in 1982 by Israel, at which point it fled to Tunisia.

In 1988, the [PLO](#) under Arafat agreed to recognise Israel and renounce terrorism. It was a historic compromise. He unilaterally surrendered Palestinian claims to 78% of historic Palestine and agreed to focus aspirations for Palestinian statehood solely on the remaining 22%, the West Bank and Gaza.

Five years later, in 1993, Arafat and Israeli Prime Minister Yitzhak Rabin signed the Oslo Accords, hailed as a blueprint for peace between the two peoples. It was the first time Israelis and Palestinians publicly recognised each other as partners for peace rather than enemies who might be defeated by force of arms. In October 1994, Israel signed a peace treaty with Jordan, leaving Syria and Lebanon the only countries bordering Israel that were still in a state of conflict with it.

The Accords created the Palestinian Authority (PA), headed by Arafat and based in Ramallah. It had limited administrative and security duties in the West Bank and Gaza while Israel still retained much control. Two years later, Rabin was assassinated by a right-wing Israeli who opposed the Oslo Accords. Rabin's replacement, Shimon Peres of the moderate Labour Party, was narrowly defeated a year later by Benjamin Netanyahu of the right-wing Likud Party. Netanyahu opposed the Accords, rejected the idea of a Palestinian state, and intensified settlement building in the occupied territories.

In July of 2000, the Labour Party was back in power, and Israeli public opinion had moved away from

Netanyahu's hard line approach, which soured relations with the Western and Arab worlds without any benefit to security. But Israelis were wary because Hamas and Islamic Jihad had committed fourteen suicide bombings during the Oslo years. And Palestinians felt betrayed because instead of retreating from the occupation as promised, the Israelis had only intensified it.

President Bill Clinton, in his final months in office, met with Israeli Prime Minister Ehud Barak and Yasser Arafat at Camp David, Maryland, for a last-ditch effort to negotiate a two-state solution. The talks failed spectacularly. From the Israeli perspective, Barak made a 'generous offer' -- including more than 90% of the West Bank and parts of East Jerusalem -- which went further than any other Israeli leader had been willing to go. Arafat rejected the deal. The result led to a Palestinian uprising and to a new Israeli Prime Minister, Ariel Sharon of the right-wing Likud party. The unrest spiraled from Palestinian protests and harsh Israeli repression into riots, suicide bombings, and massive Israeli military incursions. Israel as result in 2005 unilaterally disengaged from the Gaza Strip, evacuating settlers and its military while retaining control over most points of entry into the Gaza Strip. The election of [Hamas](#) to head the Palestinian Legislative Council in 2006 froze relations between Israel and the Palestinian Authority (PA). In 2006 Israel engaged in a 34-day conflict with [Hezbollah](#) in Lebanon in June-August 2006 and a 23-day conflict with [Hamas](#) in the Gaza Strip during December 2008 and January 2009. Prime Minister Binyamin Netanyahu formed a coalition in March 2009 following a February 2009 general election. Direct talks with the PA launched in September 2010 collapsed following the expiration of Israel's 10-month partial settlement construction moratorium in the West Bank.

As a result of the Israeli/Palestinian conflict, Israel primarily conducts financial activity outside the Middle East with the markets of the US and Europe, and, to an increasing extent, with Asia. Criminal groups in Israel, either home-grown or with ties to the former Soviet Union, US, and EU, are active. Israel's illicit drug trade is regionally focused, with Israel more of a transit country than a market destination. The majority of money laundered originates from criminal activities abroad, including "carousel fraud," which takes advantage of international value added tax loopholes. Proceeds from domestic criminal activity also continue to contribute to money laundering activity. Electronic goods, liquor, cigarettes, cell phones, and pharmaceuticals, especially Viagra and Cialis, have all been seized in recent smuggling operations. Concerns also exist about money laundering in the diamond industry, illegal online gambling rings, retail businesses suspected as money laundering enterprises, and public corruption.

Still with the Israeli Palestinian conflict still unresolved the most significant risks remain with terrorism and terrorism finance.

The Irgun - Israel / Palestine

"The National Military Organisation in the Land of Israel", or Irgun was a Zionist paramilitary group that operated in Mandate Palestine between 1931 and 1948. It was an offshoot of the earlier and larger Jewish paramilitary organisation Haganah and became a political predecessor to Israel's right-wing Herut (or "Freedom") party, which led to today's Likud party, which has led or been part of most Israeli governments since 1977. Irgun policy was based on the proposition that only with armed force by Jews would they force Arabs in Palestine to accept a Jewish State. One of the main operations for which the Irgun is best known was the bombing of the King David Hotel in Jerusalem in 1946 which as a result the Irgun became viewed as a terrorist organisation or an organisation which carried out terrorist acts. The Irgun was assimilated into the Israeli Defence Forces following the establishment of the State of Israel.

Kahane Chai - Israel

Kach, the predecessor to Kahane Chai, was founded by radical Israeli-American Rabbi Meir Kahane with the goal of restoring Greater Israel, which is generally used to refer to Israel, the West Bank, and Gaza. Its offshoot, Kahane Chai, (translation: "Kahane Lives") was founded by Meir Kahane's son Binyamin following his father's 1990 assassination in the US. Both organisations were designated as US Foreign Terrorist Organisations on October 8, 1997. The group has attempted to gain seats in the Israeli Knesset over the past several decades but has won only one seat in 1984. Kahane Chai has harassed and threatened Arabs, Palestinians, and Israeli government officials, and has vowed revenge for the death of Binyamin Kahane and his wife. The group is suspected of involvement in a number of low-level attacks since the start of the First Palestinian Intifada in 2000. Since 2003, Kahane Chai activists called for the execution of former Israeli Prime Minister Ariel Sharon, and physically intimidated other Israeli and Palestinian government officials who favored the dismantlement of Israeli settlements. Although they have not explicitly claimed responsibility for a series of mosque burnings in the West Bank, individuals affiliated with Kahane Chai are widely suspected of being the perpetrators. It receives support from sympathizers in the US and Europe.

Abergil Crime Family - Israel

Widely regarded as the foremost syndicate in Israel's mafia, the Abergil Family is today run by brothers Yitzhak and Meir Abergil. It is also considered to be among the world's top 40 largest drug importers to the US. Yitzhak and Meir were arrested and extradited to the US in 2001. According to law enforcement sources in Israel the family's syndicate is reported to have continued operations in the absence of its leaders, though in August of 2011 Meir Abergil was permitted to return to Israel after plea negotiations with US officials.

Alperon Crime Family - Israel

The Alperon crime family rose to prominence under the leadership of Yaakov Alperon. Yaakov and his brothers

established a protection racket and conducted widespread extortion. In 1993 Yaakov was jailed for four and a half years, while two of his brothers faced similar convictions. The Alperon family was also involved in long term feuding with other Israeli mafia groups, including Zeev Rosenstein, as well as the Abutbul and Abergil families in disputes surround the bottle recycling industry. These bottles acted as a covert form of payment in a protection racketeering scheme, as the bottles could be exchanged for cash. In 2006, at a meeting held between Israeli mafia leader Amir Mulner and Yaakov Alperon in order to resolve a dispute, Alperon reportedly stabbed Mulner in the neck and Yaakov Alperon and his son went into hiding. In 2008 Yaakov Alperon was assassinated, killed by a bomb blast detonated in his car. The chief suspect is believed to be Mulner. At his father's funeral one of Alperon's sons is reported to have sworn revenge, promising that: "We will find the man who did this. I'll send this man to God. He won't have a grave because I'll cut off his arms, his head, and his legs."⁹⁹

Zeev Rosenstein Organisation - Israel

Zeev Rosenstein was a leading crime boss in Israel until his arrest in 2004.¹⁰ Rosenstein was charged with distributing ecstasy in the US after the seizure of 700,000 ecstasy tablets in Manhattan. Prior to his arrest Rosenstein had been engaged in the feuding between rival Israeli syndicates and had survived seven attempts on his life, earning him the name "wolf with seven lives" (Zeev meaning wolf in Hebrew).

Palestine Liberation Organisation (PLO) - Palestine

The Palestine Liberation Organisation (PLO) is a political and paramilitary organisation which was created in 1964, recognised as the "sole legitimate representative of the Palestinian people" by the UN and over 100 states with which it holds diplomatic relations. The PLO was considered by the US and Israel to be a terrorist organisation until 1991. In 1993, the PLO recognised Israel's right to exist in peace, accepted UN Security Council resolutions 242 and 338, and rejected "violence and terrorism"; in response, Israel officially recognised the PLO as the representative of the Palestinian people. Yasser Arafat was the Chairman of the PLO Executive Committee from 1969 until his death in 2004. He was succeeded by Mahmoud Abbas (also known as Abu Mazen). Initially, as an armed guerrilla organisation, the PLO was responsible for terrorist activities performed against Israel in the 1970s and early 1980s. In 1988, however, the PLO officially endorsed a two-state solution, contingent on terms such as making East Jerusalem capital of the Palestinian state and giving Palestinians the right of return to land occupied by Palestinians prior to 1948, as well as the right to continue armed struggle until the end of "The Zionist Entity." In 1996, the PLO nullified the articles of the PLO's Charter, or parts of it, which called for the destruction of Israel and for armed resistance. The PLO has numerous factions though the top 3 include; Fatah which is the largest faction, and was the faction led by Yasser Arafat, (with sub-factions or armed wings or splinter groups from

Fatah including: Black September; Al-Aqsa Martyrs Brigade and Tanzim; the Popular Front for the Liberation of Palestine (PFLP), the second largest faction, the Democratic Front for the Liberation of Palestine (DFLP) the third largest. Abu Nidal, although no longer active split from the PLO in 1974.

Fatah - Palestine

Fatah is a secular Palestinian nationalist organisation that has played, and continues to play, a pivotal role in Palestinian politics. Fatah was originally founded in 1959 by 5 Palestinian activists operating out of Kuwait: Yasser Arafat, Khalil El-Wazir, Salah Khalaf, Khalid al-Hasan, and Faruk Qaddumi. Fatah was the first Palestinian group to openly call for a direct conflict with Israel. From a base focussed solely on violent resistance to Israel and over time with increasing popularity and membership Fatah expanded its sphere of activity to include civil and social affairs. This move allowed Fatah to create a broad popular base for its organisation, which though affiliated with the violent struggle, in truth had little or no involvement with the violent attacks perpetrated by the organisation's more martial elements. Following the Arab defeat in the 1967 Arab-Israeli War (a conflict fought between Israel and the Arab states of Egypt, Jordan and Syria), Fatah aligned itself with the PLO and soon came to dominate the organisation. By the time the 1960s came to a close Fatah had succeeded in securing the support of several Arab and Eastern-bloc states, and by 1974 a Fatah dominated PLO had been officially recognised by the Arab summit and the UN.

During the intifada, a mass protest that broke out in late 1987, the Fatah dominated PLO again demonstrated its capacity for non-violence and attempted to use the unrest to press for a peace settlement with Israel. It is therefore important to recognise that the history of Fatah has not been exclusively violent, but rather a campaign that has swung frequently between an emphasis on violent uprising, and peaceful social regeneration. As a result of Fatah and the PLO's move towards a settlement in late 1988 a dialogue was established between the warring factions in Israel and Palestine; a dialogue that led directly to the 1993 Oslo Accords. As part of the milestone agreement all PLO factions, including Fatah, recognised the State of Israel and renounced acts of terrorism. Since 1993, the PLO has transformed itself into a quasi-government, the Palestinian Authority (PA) with Arafat and Fatah still playing the dominant roles. While Fatah and Arafat formally committed themselves to working with Israel towards peace, the reality has been much more complicated. Many Fatah members are actively engaged in legitimate Palestinian Authority governmental activities, however certain factions within Fatah have re-committed themselves to violence. Notably, the al-Aqsa Martyrs Brigades and the Fatah-Tanzim have been implicated in terrorist activities against Israeli targets. While Fatah leaders maintain that these factions operate autonomously, beyond the control of the mainstream movement, Israel accuses Fatah not only of condoning, but also of controlling these militant

activists. Irrespective of whether such allegations hold any veracity, there exists an undeniable fissure between Fatah's traditional role as the source of violent Palestinian resistance and its more recent function as a governmental institute.

Since 2005 however, Fatah's influence as a political party has waned considerably, largely as a result of internal dissension, and the organisation was replaced in 2006 by Hamas as the governing party. Factional clashes in the Gaza strip between supporters of the two political entities following this transition have claimed lives on both sides. Today, whilst the State of Palestine was declared as an Independent State in 2013, Fatah effectively leads in the West Bank and Hamas in the Gaza Strip, whilst Israel continues to dominate and dictate the terms of co-existence.

Al-Aqsa Martyrs Brigades - Palestine

Designated as a US Foreign Terrorist Organisation on March 27, 2002, the al-Aqsa Martyrs Brigade is composed of an unknown number of small cells of Fatah-affiliated activists that emerged at the outset of the al-Aqsa Intifada, in September 2000. Al-Aqsa's goal is to drive the Israeli military and West Bank settlers from the West Bank in order to establish a Palestinian state loyal to Fatah. Al-Aqsa employed primarily small-arms attacks against Israeli military personnel and settlers as the intifada spread in 2000, but by 2002 they turned increasingly to suicide bombings against Israeli civilians inside Israel. In January 2002, the group claimed responsibility for the first female suicide bombing inside Israel. In 2010, The group continues to launch rocket attacks on communities in Israel. Most of al-Aqsa's operational activity is in Gaza but the group also planned and conducted attacks inside Israel and the West Bank. The group also has members in Palestinian refugee camps in Lebanon. Iran has exploited al-Aqsa's lack of resources and formal leadership by providing funds and guidance, mostly through Hezbollah facilitators. The AAMB has since become known as the al-Sha'id Yasser Arafat Brigades.

Tanzim - Palestine

The Tanzim militia, were founded in 1995 by Yasser Arafat and other Fatah leaders to counter Palestinian Islamism and is widely considered to be an armed offshoot of Fatah with its own leadership structure. The acknowledged head of the Tanzim is Marwan Barghouti, who is as of 2010, serving five consecutive life sentences in Israel for murder, and, according to some accounts, has a substantial following among the "rejectionist" camp which opposes the Interim Agreement/Oslo accords signed on 28 September 1995 with Israel. Tanzim came to prominence in the street fighting which marked the beginning of the second Palestinian Intifada. Its members tend to be younger than those of other Fatah factions, often having grown up in the post-Oslo era. Many Tanzim members have joined the al-Sha'id Yasser Arafat Brigades (formerly the al-Aqsa Martyrs' Brigades). Tanzim has also recruited female suicide bombers,

including Andaleeb Takatka, a 20-year-old Bethlehem woman who detonated an explosive belt at a Jerusalem bus stop in April 2002, killing six Israeli civilians, and injuring sixty. The exact nature of the relationships between the Tanzim, Fatah leadership and the al-Aqsa Martyrs Brigades (now al-Shaid) remains unclear. Fatah's leadership has publicly renounced terrorist activity and claims that the Tanzim and the Yasser Arafat Brigades operate independently. Many terrorist attacks within Israel and the Occupied Territories, however, were still reported as being the work of al-Fatah in general. Tanzim is known to have run summer training camps and instilled a high level of discipline in its predominantly college aged recruits. Aside from its military exploits, the organisation also operates at the grassroots level, cultivating support in neighbourhood cells. In the early 2000s the group claimed a membership of 10,000 mainly in Gaza and the West Bank, though the number of active militants is undoubtedly considerably less than this. According to an Israeli Defence Forces spokesperson, Tanzim militants are believed to have equipped themselves with German MP-5 submachine guns smuggled into Palestine from Jordan and Egypt. In terms of ideology Tanzim has followed the political and spiritual direction of Arafat throughout his political career. Prior to his death in 2004 it had however been questioned whether Arafat still maintained control over this powerful militia. Since the rise to power of Hamas in the Gaza strip, tensions have mounted between militia's aligned with al-Fatah, and those allied to Hamas. However in 2011 a reconciliation agreement was signed, and in 2013 the two parties met in Cairo in an attempt to make a deal. After a first round of discussions lasting 8 hours, the outcome of the second round has yet to emerge.

Black September - Palestine

The Black September Organisation (BSO) came into existence in 1971, professing itself to be a distinct splinter group from Fatah. The self-proclaimed objective of the group was to avenge the expulsion of the Palestine Liberation Organisation (PLO) from Jordan in September of 1970. This expulsion of the PLO became known as "Black September," a period from which the group derived its name. Despite purporting to be an autonomous splinter group, enduring connections with Fatah were revealed following the arrest of BSO operatives. It emerged that rather than a breakaway faction, BSO was in fact the creation of Fatah as a means of continuing operations in other Arab nations without implicating itself at a time when it had declared that it would not interfere in the domestic situations of neighbouring Arab nations. The operational period of the BSO was relatively brief, lasting in total three years until the end of 1973, however during this time the terrorist attacks perpetrated were of international significance. Particularly infamous was the BSO's attack on Israeli Olympians in Munich in 1972, in which 11 athletes perished. As a result the BSO suffered a severe backlash from Israeli security forces bent on eradicating the group. In

1974, having sustained heavy losses, Black September was disbanded by Fatah. The group's members did not however simply fade into obscurity, with attacks continuing in the organisation's name for some time following its official dissolution. Many BSO members were also absorbed by other terrorist organisations such as the Popular Front for the Liberation of Palestine (PFLP). Today the group is now considered inactive.

Abu Nidal Organisation - Palestine

The Abu Nidal Organisation (ANO) was an infamous Palestinian terrorist group who split from the Palestinian Liberation Organisation (PLO) when the latter proposed the creation of the Palestinian National Authority in 1974. Group leader Sabri al-Banna aka Abu Nidal believed that no goal other than the total liberation of the Palestinian people was acceptable and that the only method by which to accomplish that goal was armed struggle. Abu Nidal bore a deep-seated hatred for Israel ("It is a crime to allow the Zionists to leave our land alive"), the US ("Were it not for American support, the Zionist ghost would have long vanished from the world arena") and Arab leaders who have engaged politically with Israel or the West. Abu Nidal sometimes referred to these leaders as "Zionists who are not Jews," and they became the target of many ANO attacks

The Abu Nidal Organisation, despite its vehement use of the Zionist label for its enemies, was not in fact a religious group. Rather Sabri al-Banna was primarily motivated by anger over the displacement of his family from Palestinian land during the 1948 Israeli War of Independence. The peak of the ANO's power was reached during the 1980s, at which point terrorism experts deemed it to be the foremost international terrorist organisation in the world. With as many as 400 members, along with a plethora of different organisation names (a subterfuge intended to portray ANO operations as the work of disparate groups), at the height of its operational power the ANO boasted a sophisticated internal structure. For instance in 1985 the ANO established its Intelligence Directorate, beneath which resided four sub-committees: the Committee for Special Missions, The Foreign Intelligence Committee, the Counter-Espionage Committee, and the Lebanon Committee. It was therefore, at least in designation, a structure highly reminiscent of many western government security services. The Committee for Special Missions was responsible for selecting suitable targets for ANO attacks and would compile short-lists to be reviewed by Abu Nidal and committee's head al-Ali. It was however the Intelligence and Espionage elements of the ANO, and indeed of Abu Nidal's psyche, that proved to be the organisation's undoing. By 1987, at the behest of Abu Nidal, the ANO had turned its intelligence apparatus inwards, focusing on the suspected plots and deceptions of its own members. The consequences of this internal scrutiny and for the most part paranoia were astounding; in one night in November 1987 some 170 ANO members were executed and concealed in a mass grave. Soon after a further 160 members met a similarly

gruesome end in Libya, considerably weakening the international capabilities of the group.

The finances of the ANO are believed to have been derived primarily from the government sponsorship of Syria, Libya, and Iraq. In Libya, Nidal built a close personal relationship with then leader Muammar Gaddafi, from whom he gained a great deal of support. This patronage however came to an end when Libyan connections to the Lockerbie bombing emerged, after which Gaddafi expelled Abu Nidal from Libya in an attempt to separate himself from the politically damaging image of terrorism. Arguably the most prominent terrorist strike made by the ANO during its operational years was its simultaneous attack on the airports of Rome and Vienna in 1985.¹¹ In the Leonardo Da Vinci International Airport in Rome ANO gunmen opened fire at Israel's El Al ticket kiosk killing 16 people and injuring 99 others. Minutes later in Vienna International Airport hand grenades were aimed at passengers waiting to board a flight to Tel Aviv, resulting in 2 fatalities and 39 injuries. The purpose of these attacks is believed to have been to damage prospects of Israeli-Palestinian peace talks; a process with which the Italian and Austrian governments were closely involved. However since the late 1980s the ANO has not attacked a Western target, and in August of 2002 the Iraqi government claimed that Abu Nidal had committed suicide in Iraq. Speculation continues to circulate around the true circumstances of Nidal's death, with many believing that Saddam Hussein ordered his assassination, while others contend that Nidal is not really dead. In 2008 a report was published by The Independent's Middle East Correspondent Robert Fisk after reportedly gaining access to Iraqi files indicating that Abu Nidal had undergone interrogation by Iraqi intelligence officers prior to his death. The remaining leadership of the organisation has publicly stated that the ANO did not die with its founder and that a new leader will be named. Irrespective of this claim it is thought to be highly unlikely that the group will reactivate

Popular Front for the Liberation of Palestine (PFLP) - Palestine

PFLP is a Marxist-Leninist group founded in 1967 by George Habash as a member of the PLO, advocating a Pan-Arab revolution. The group earned a reputation for spectacular international attacks in the 1960s and 1970s, including airline hijackings that killed many. A leading faction within the PLO, the PFLP has long accepted the concept of a two-state solution but has opposed specific provisions of various peace initiatives. The PFLP opposed the Declaration of Principles signed in 1993 and suspended its participation in the PLO. It committed numerous international terrorist attacks during the 1970s. Since 1978 PFLP has carried out numerous attacks against Israeli or moderate Arab targets, including the killing of a settler and her son in December 1996. It receives most of its financial and military assistance from Syria and Libya. The PFLP stepped up its operational activity during the Second Intifada. This

was highlighted by at least two suicide bombings since 2003, multiple joint operations with other Palestinian terrorist groups, and the assassination of Israeli Tourism Minister Rehavam Ze'evi in 2001, to avenge Israel's killing of the PFLP Secretary General earlier that year. The PFLP was involved in several rocket attacks, launched primarily from Gaza, against Israel in 2008 and 2009, and claimed responsibility for numerous attacks on Israeli forces in Gaza, including a December 2009 ambush of Israeli soldiers in central Gaza. The PFLP claimed numerous mortar and rocket attacks fired from Gaza into Israel in 2010, as well as a February attack on a group of Israeli citizens. In 2011, the group continued to use rockets and mortars to target communities in Israel.

Democratic Front for the Liberation of Palestine (DFLP) - Palestine

The Democratic Front for the Liberation of Palestine was formed from a break from PFLP in 1969. It called for more Maoist and a non-Nasserist approach and demanded a socialist policy and alignment of the Arab world, drawing models from China, Vietnam and Cuba. Despite its criticism of Arafat, DFPL has always supported PLO unity; It believes Palestinian national goals can be achieved only through the revolution of the masses. It opposed the Declaration of Principles (DOP) signed in 1993. In the early 1980s it occupied a political stance midway between Arafat and the rejectionists. It split into two factions in 1991, one pro-Arafat and another more hardline faction headed by Nayif Hawatmah (which suspended its participation in the PLO). In the 1970s it carried out numerous small bombings and minor assaults and some more spectacular operations in Israel and the occupied territories, concentrating on Israeli targets. It is involved only in border raids since 1988, but continues to oppose the Israel-PLO peace agreement. It received financial and military aid from Syria and Libya.

Palestine Islamic Jihad (PIJ) - Palestine

The PIJ originated among militant Palestinians in the Gaza Strip during the 1970s and is sometimes known as the Al-Quds Brigades. Committed to the creation of an Islamic Palestinian state and the destruction of Israel through holy war. Because of its strong support for Israel, the US has been identified as an enemy of the PIJ, but the group has not specifically conducted attacks against US interests in the past. In July 2000, however, it publicly threatened to attack US interests if the US Embassy was moved from Tel Aviv to Jerusalem. Also it opposes moderate Arab governments that it believes have been tainted by Western secularism. It has conducted at least three attacks against Israeli interests in late 2000, including one to commemorate the anniversary of former PIJ leader Fathi Shqaqi's murder in Malta on 26 October 1995. It conducted suicide bombings against Israeli targets in the West Bank, Gaza Strip, and Israel. PIJ attacks in 2008, 2009, and 2010 were primarily rocket attacks aimed at southern Israeli

cities, but also included attacking Israeli targets with explosive devices. PIJ continued operations into 2011, claiming responsibility for a mortar attack in Sderot, Israel in February, and a rocket attack in Ashdod, Israel in March. It receives financial assistance and training primarily from Iran

Palestine Liberation Front (PLF) - Palestine

The PLF broke away from the PFLP in the mid-1970s and later would split again into pro-PLO, pro-Syrian, and pro-Libyan factions. Pro-PLO faction led by Muhammad Abbas (Abu Abbas), who became a member of PLO Executive Committee in 1984 but left it in 1991. The Abu Abbas-led faction is known for aerial attacks against Israel. Abbas' group also was responsible for the attack in 1985 on the cruise ship Achille Lauro and the murder of US citizen Leon Klinghoffer. After going approximately 16 years without claiming responsibility for an attack, the PLF claimed responsibility for two attacks against Israeli targets in 2008. One attack was against an Israeli military bus in Huwara, Israel, and the other involved a PLF "brigade" firing at an Israeli settler south of the Hebron Mountain, seriously wounding him. On March 28, 2008, shortly after the attacks, a PLF Central Committee member reaffirmed PLF's commitment to using "all possible means to restore" its previous glory and to adhering to its role in the Palestinian "struggle" and "resistance," through its military.

Army of Islam (AOI) - Palestine

The Army of Islam is a Gaza-based terrorist organisation founded in late 2005 that has been responsible for numerous terrorist acts against the Governments of Israel and Egypt, as well as American, British, and New Zealander citizens. AOI is led by Mumtaz Dughmush, and operates in Gaza. It subscribes to a Salafist ideology together with the traditional model of armed Palestinian resistance. AOI has previously worked with Hamas and is attempting to develop closer Al-Qaeda contacts. AOI's terrorist acts include a number of rocket attacks on Israel, the 2006 kidnapping of two journalists in Gaza (an American and a New Zealander), and the 2007 kidnapping of a British citizen, journalist Alan Johnston, in Gaza. AOI is also responsible for early 2009 attacks on Egyptian civilians in Cairo and Heliopolis, Egypt. AOI is alleged to have planned the January 1, 2011 Alexandria attack on a Coptic Christian church that killed 25 and wounded 100. On May 7, 2011, the group released a eulogy for bin Laden via its Al Nur Media Foundation. AOI receives the bulk of its funding from a variety of criminal activities in Gaza. It was designated a US Foreign Terrorist Organisation on 19 May 2011.

Hizb-ut-Tahrir - Palestine/Global

Hizb ut-Tahrir or Party of Liberation is an international pan-Islamic political organisation. They are commonly associated with the goal of all Muslim countries uniting as an Islamic state or caliphate ruled by Islamic law and with a caliph head of state elected by Muslims. The organisation was founded in 1953 as a Sunni Muslim

organisation in Jerusalem by Taqiuddin al-Nabhani, an Islamic scholar. Since then Hizb ut-Tahrir has spread to more than 40 countries and by one estimate has about one million members. Hizb ut-Tahrir is very active in the West, particularly in the United Kingdom, and is also active in several Arab and Central Asian countries, despite being banned by some governments, including by the Russian Government and many in the middle east. The group also has a growing presence in North America, known as Hizb ut-Tahrir America, or HTA. Hizb ut-Tahrir believes the re-establishment of caliphate would provide stability and security to both Muslims and Non-Muslims in the predominantly Muslim regions of the world. The party promotes a detailed program for the institution of a caliphate that would establish Shariah and carry "the Da'wah of Islam" to the world. Hizb ut-Tahrir is also strongly anti-Zionist and calls for Israel, which it calls an "illegal entity," to be dismantled.

Whilst Hizb ut-Tahrir's is officially opposed to violence this has often been questioned. For example, the think tank GlobalSecurity.org states that Hizb ut-Tahrir "is not against violence as such. It is just against the use of violence now." Zeyno Baran of the Nixon Center and Ariel Cohen of the Heritage Foundation have argued that although Hizb ut-Tahrir does not promote or engage in violence, it acts as a "conveyor belt" for young Muslims, using its legal status to indoctrinate them before they leave the group to join more extreme groups that may engage in violence.

An investigative journalist specialising in British terrorism, Shiv Malik sympathizes with the position, stating that it "is not without foundation." In support of this perspective, Malik quotes unnamed intelligence sources stating that Abu Musab al-Zarqawi, a leader of Al-Qaeda in Iraq, and Al-Qaeda leader Khalid Sheikh Mohammed are both former members of Hizb ut-Tahrir. Omar Sharif, who attempted a suicide bombing in Israel in 2003, is also alleged to have been affiliated with Hizb ut-Tahrir, but the group denies this, stating that "despite extensive investigations by the police and security services, including legal proceedings against members of the Sharif family, no link to Hizb ut-Tahrir has ever been proven." The British government, in a classified report, discounted the conveyor belt theory, stating "We do not believe that it is accurate to regard radicalisation in this country as a linear 'conveyor belt' moving from grievance, through radicalisation, to violence ... This thesis seems to both misread the radicalisation process and to give undue weight to ideological factors."

Special Focus 4

Hamas - Palestine



Founded in 1987 during the First Intifada, Hamas represents a violent splinter group of the Muslim Brotherhood is a religious movement adhering to the Sunni sect of the Islamic faith, which began its political activity in Egypt and focussed primarily on non-violent activism. The new and altogether more violent Hamas (the word translates to mean 'zeal') was established by Sheik Ahmed Yassin, a man who had formerly participated in a great deal of non-violent work aimed at social regeneration in the Palestinian territories and who had directed Muslim Brotherhood activities in the area. However, by the 1980s Yassin had begun to favour a combined approach of social aid, political activity, and violent action.

Hamas' social services division, which includes charities, schools, youth camps, fund raising and medical clinics, is known as the "Dawa." This body has proved highly effective in creating a popular base of support for Hamas, supporting many vulnerable groups, operating largely free of corruption and as a result acting as an effective means of recruitment. The Dawa in particular has allowed Hamas to project a form of legitimacy at least with some, for example whilst the US and Israeli governments designate Hamas in its entirety as a Terrorist Organisation, the EU lists only the military wing of Hamas and not its so called social wing. The military wing of Hamas is known as the Izz ad-Din al-Qassam Brigades and has been responsible for numerous attacks against both civilian and military targets. These attacks first began in 1987, and included not only Israeli targets, but also Israeli collaborators within Palestinian society. The organisation's first suicide bombing was undertaken in April of 1993, detonating a roadside bomb near Mehola in the West Bank. Such attacks have since become characteristic of the group's operations.

Up until 2005, Hamas conducted numerous anti-Israeli attacks, including suicide bombings, rocket launches, improvised explosive device (IED) attacks, and shootings, contributing significantly to many deaths and injuries in the Second Intifada killings (2000-2004) and though Hamas has not directly targeted non-Israeli targets or interests, the group makes little or no effort to avoid collateral damage to foreigners. Hamas suspended terrorist attacks in February 2005, though has been responsible for rocket fire into Israel since.

Hamas probably has several hundred operatives in its armed wing, the al-Qassam Brigades, along with its

reported 9,000-man Executive Force and tens of thousands of supporters and sympathizers. Hamas has an operational presence in every major city in the Palestinian territories and currently focuses its anti-Israeli attacks on targets in the West Bank and within Israel. The group retains a cadre of leaders and facilitators that conducts diplomatic, fundraising, and arms smuggling activities in Lebanon, Syria, and other states. Hamas is also increasing its presence in the Palestinian refugee camps in Lebanon, probably with the goal of eclipsing Fatah's longtime dominance of the camps. Hamas receives some funding, weapons, and training from Iran. In addition, fundraising takes place in the Gulf countries, but the group also receives donations from Palestinian expatriates around the world and private benefactors in Arab states. Some fundraising and propaganda activity takes place in Western Europe and North America. Charities have also been a significant source of financing for Hamas including from the [Holy Land Foundation](#), the [Al-Aqsa Foundation](#), [Interpal](#), [Association de Secours Palestiniens](#), [Comité de Bienfaisance et de Secours aux Palestiniens](#), the [Palestinian Association of Austria](#) and the [Sanabel Association for Relief and Development](#). US Plaintiffs' groups involved in litigation have claimed that [Hamas](#) receives "funding" from a global family of charities established by the [Muslim Brotherhood](#) under the umbrella of the Union of Good.

The political or "Shura Council" that oversees all Hamas operations and is responsible for all major decision making established its headquarters abroad first in the US, then Jordan and then Syria, before establishing itself firmly now in Gaza, following its victory in first winning control of the PA legislature and cabinet in January 2006. Following the election the US and EU ceased to provide financial aid to the Palestinian government in response to the new administration's failure to accept past peace agreements with Israel. The transition in political power led to a direct conflict between Hamas and Fatah in 2007 known as the Battle of Gaza. Despite receiving aid from the US and Israel, Fatah forces were defeated in the Gaza Strip, and two de-facto governments have arisen within Palestine. Hamas continues to govern the Gaza strip led by Prime Minister Ismail Haniyeh, while Fatah governs the West Bank and has in 2013 renamed itself the State of Palestine. Reconciliation between the two groups has yet to be reached, though economic links have been maintained between the two areas.

While Hamas is very much distinct from Al-Qaeda as an organisation, investigators report links between the Muslim Brotherhood (from which Hamas emerged) and AQ, and suggest that AQ cells have supplied funds to Hamas. The Sunni denomination adopted by Hamas has also made the group widely appealing to many Islamist groups in North Africa. Hamas might therefore be viewed as a localised expression of a larger picture, in which an increasing fusion of religion (particularly Islam) and politics has emerged with greater vitality across much of the Middle East and North Africa.

Syria



Following World War I, France acquired a mandate over the northern portion of the former Ottoman Empire province of Syria administering the area as Syria until granting it independence in 1946. The new country lacked political stability, however, and experienced a series of

military coups during its first decades. Syria united with Egypt in February 1958 to form the United Arab Republic. In September 1961, the two entities separated, and the Syrian Arab Republic was re-established. In the 1967 Arab-Israeli War, Syria lost the Golan Heights to Israel. The current regime is led by Bashar al-Assad who succeeded his father after he died in 2000. The modern Syria was founded by Hafez al-Assad and is dominated by Alawite Muslims, which is an offshoot of the Shi'ite branch of Islam. The Alawites are a minority in Syria, but dominate the government and the military. Hezbollah, based in neighboring Lebanon and which depends on the Assad regime and Iran for finance and weapons, has crossed into Syria and joined the battle against the rebels. International pressure on the Assad regime has intensified since the start of the Arab Spring in late 2011, as the Arab League, EU, Turkey, and the US have expanded sanctions as a full blooded civil war rages in Syria. Numerous groups are battling it out against the government's security forces backing the Al-Assad regime in many areas of the country. The civil war has escalated with charges against the regime of using chemical weapons on civilians. On the opposition side, the main combatants are the Free Syrian Army, the Syrian Islamic Liberation Front, Jabhat al-Nusra, the Syrian Islamic Front, the Al-Nusra Front; the Islamic State of Iraq and Syria (ISIS). The Free Syrian Army is considered the most moderate of the opposition groups. The relatively moderate force emerged from the street protests and initial Syrian army defections to take on Assad's force, and are made up largely of Sunni Muslims, who are a majority in Syria, but is badly divided among different factions.

Syrian Islamic Liberation Front - Syria

The Syrian Islamic Liberation Front is probably the largest of the armed opposition groups and works alongside the Free Syrian Army. Founded in September 2012 after secret negotiations between the group's leaders, the group is headed by Ahmed Eissa al-Sheikh, the leader of the Suqour al-Sham Brigade. The coalition includes around 20 groups and has tens of thousands of fighters active throughout much of Syria, with the most important being the Suqour al-Sham Brigade (Idlib), Farouq Brigade (Homs), Liwa al-Islam (Damascus) and Tawhid Brigade (Aleppo). The group has an Islamist ideology. It

includes both Muslim Brotherhood and Salafist inspired groups, however the group is not seen as hardline as either the Syrian Islamic Front or the al-Nusra Front, and far removed from ISIS.

Syrian Islamic Front - Syria

The Syrian Islamic Front or al-Jabhab al-Islamiyya as-Suriyah is a Salafist umbrella organisation of Islamist rebel groups. It may now also be operating as Harakat Ahrar al-Sham al-Islamiyya (The Islamic Movement of Ahrar al-Sham). Its largest group is the Salafist Ahrar al-Sham, which reportedly "leads" and "dominates" the Front. The group was founded by eleven Islamist rebel groups including: Ahrar al-Sham, Al-Haqq Brigade in Homs, the Al-Fajr Islamic Movement in Aleppo, Ansar Al-Sham in Latakia, Jaysh Al-Tawhid in Deir ez-Zor and the Hamza ibn 'Abd al-Muttalib Brigade in Damascus. The Group does not include the jihadist Al-Nusra Front, though is prepared to work with other opposition groups including with the Front.

Al-Nusra Front/Jubhat al-Nusra - Syria

The Al-Nusra Front or Jubhat al-Nusra is a radical Islamic force that has pledged allegiance to Al-Qaeda, has attracted thousands of militant Muslims from around the world, received money and weapons from supporters, and has become one of the rebels' most effective fighting force. It is imposing Sharia law in areas it occupies and has also skirmished with the Free Syrian Army, at times. The Front has been designated by the UN, US, UK, and Australia as a terrorist organisation.

The Islamic State of Iraq and Syria (ISIS) - Syria

The Islamic State of Iraq and Syria (ISIS) also known as The Islamic State of Iraq and the Levant is led by Abu Bakr al-Baghdadi and emerged out of the Al-Nusra Front in 2013 based on a request, it is thought, by Al-Qaeda leader Ayman al-Zawahri to set up an Islamic state in the region. Despite its loyalty to Al-Qaeda, the Al-Nusra Front did not obey the request at the time. The ISIS is made up largely of foreign fighters looking beyond Syria to establish an Islamic Caliphate joining, first Iraq and Syria, whereas the Al-Nusra Front is interested at this stage at least only in the future of Syria. ISIS is supported by and can be considered a sister organisation of AQ in Iraq, with some believing ISIS a rebranded version of AQ in Iraq, to reflect its growing ambitions in the region. It is concentrated mostly in the northern and eastern provinces of the country and with its radical ideology and tactics such as kidnappings and beheadings, the group has stamped its identity on the communities in which it is present, including, crucially, areas surrounding the main border crossings with Turkey. It has been bolstered by an influx of thousands of foreign fighters from the region and beyond.

Syria is subject to increasing Sanctions and Embargoes. For more information on these see Part 1, Section 3, Money Laundering Laws & Regulations; Sanctions & Embargoes above.

Lebanon



After the fall of the Ottoman Empire, after World War I, the League of Nations put Syria under a French mandate who designated what is today's Lebanon which declared independence in 1943. Since independence the country has been marked by periods of political turmoil interspersed with prosperity built on its position as a regional center for finance and trade.

The country's 1975-90 civil war that resulted in an estimated 120,000 fatalities, was followed by years of social and political instability. Sectarianism is a key element of Lebanese political life. Neighboring Syria has long influenced Lebanon's foreign policy and internal policies, and its military occupied Lebanon from 1976 until 2005.

The Lebanon-based Hezbollah militia and Israel continued attacks and counterattacks against each other after Syria's withdrawal, and fought a brief war in 2006. Lebanon's borders with Syria and Israel remain unresolved.

Jund al-Sham - Lebanon / Syria

Jund al-Sham, also known as the Army of the Levant and the Soldiers of Greater Syria, originally established in 1999 in Afghanistan with contacts with Al-Qaeda with new groups resurfacing in 2004 and 2005. Following the US military intervention in Afghanistan, Jund al-Sham was widely scattered and many of its members are believed to have returned to their homelands where other groups operating under the same title surfaced in 2004 and 2005. It is unclear whether the 2004 incarnation in the Lebanon is in fact closely connected with the Asbat al-Ansar. In 2005, a third Jund al-Sham emerged in Damascus and instantly became a highly publicized target of Syrian security authorities. Although the connection between any or all of the Jund al-Sham entities is unclear, they all continue to clash with security elements and rival factions in their respective areas of operation in order to achieve the unified purpose of replacing what they view as misguided forms of Islam and governmental rule with their vision of a traditional Islamic caliphate extending across the Levant, and are considered under the greater Al-Qaeda umbrella and therefore may be expected to remain active in various forms and guises throughout the region. The group is designated as a terrorist organisation by Russia.

Amal - Lebanon

Amal was formed in 1975 by the Iranian Imam Musa Sadr. Despite the founder's Iranian heritage, Amal was

expressly formed to protect and increase the influence of Lebanon's Shi'ite Muslim population. In addition, the group was interested in establishing a theocratic Islamic state. The group's name, Amal, has a double meaning. While Amal means "hope" in Arabic, it also represents an acronym of "Afwaj al Muqawama al Lubnaniya," or in English, "Lebanese Resistance Detachments. In 1974, Musa Sadr founded the "Movement of the Deprived" to advance the political interests of the Shi'ites in Lebanon. Upon the outbreak of Lebanon's civil war in 1975, Musa Sadr established Amal as the military wing of the Movement of the Deprived. Amal would eventually kill dozens through its terrorist attacks. Amal gained legitimacy with an increasing number of Lebanese Shi'ites after Israel's invasion of Lebanon in 1978 and the accompanying clashes between Israelis and Palestinians in southern Lebanon. With the death of Musa Sadr in 1978, Amal's leadership passed to Nabih Berri, a secular politician. Consequently, Berri was more interested in the nationalist goals of the Lebanese Shi'ites rather than any objective to create a theocratic Islamic state. Despite Berri's secularism, Amal benefited from the 1978-1979 Iranian revolution. From 1979 to 1982, Amal received financial assistance from Iran. In 1982, Iran founded Hezbollah to counter the Israeli forces that had entered Lebanon to destroy the PLO's Lebanese base. With Hezbollah's founding, Amal lost Iran's financial backing. In 1985, Syria initiated financial assistance to Amal. Amal's significance has decreased substantially since its founding. The death of Musa Sadr, the group's founder and the rise of Hezbollah have weakened the group.

Asbat al-Ansar (AAA) - Lebanon

Asbat al-Ansar is a Lebanon-based Sunni extremist group composed primarily of Palestinians with links to Al-Qaeda and other Sunni extremist groups. Asbat al-Ansar was designated as a US Foreign Terrorist Organisation on 27 March 2002. Some of the group's stated goals include thwarting perceived anti-Islamic and pro-Western influences in the country, although the group remains largely confined to Lebanon's refugee camps. Asbat al-Ansar first emerged in the early 1990s. In the mid-1990s, the group assassinated Lebanese religious leaders and bombed nightclubs, theaters, and liquor stores. The group has also plotted against foreign diplomatic targets. In October 2004, Maher al-Sa'di, a member of Asbat al-Ansar, was sentenced, in absentia, to life imprisonment for his 2000 plot to assassinate then-US Ambassador to Lebanon David Satterfield. Asbat al-Ansar has no formal ties to the AQ network, but the group shares AQ's ideology and has publicly proclaimed its support for Al-Qaeda in Iraq. Members of the group have traveled to Iraq since 2005 to fight Coalition Forces. Asbat al-Ansar has been reluctant to involve itself in operations in Lebanon due in part to concerns over losing its safe haven in Ain al-Hilwah. The group's primary base of operations is the Ain al-Hilwah Palestinian refugee camp near Sidon in southern Lebanon. It is likely that the group receives money through international Sunni extremist networks.

Special Focus 5

Hezbollah - Lebanon



Although originating in earlier formations, Hezbollah as we know it today was established in 1982 in response to the Israeli occupation of Lebanon. The name Hezbollah literally means the 'Army of God' in Arabic and is a Shiite-dominated political party in Lebanon. Its greatest enemy is Israel, which Hezbollah has refused to acknowledge as a lawful state. Hezbollah has three main goals (i) the eradication of western colonialism in Lebanon; (ii) the upholding of justice for those who have been oppressed; (iii) the transformation of Lebanon into an Islamic state. However, this final aspiration has been deemed impractical and temporarily aborted. Hezbollah is said to have gained strong support in these endeavours from Iran and Syria. In recent years, Hezbollah has expanded its primary activity i.e. military operations, to encompass political and social development in Lebanon. In the 2005 Lebanese General Election, Hezbollah managed to secure 10.9% of the seats in the Lebanese Parliament. It has also participated extensively in social development programmes in Lebanon, such as operating hospitals and clinics, building schools and providing technical assistance in the agricultural sector.

Hezbollah gained its notoriety from its fundamentalist philosophies and the tactics deployed in the liberation of Lebanon during the Israeli occupation in the 1980s. For some, Hezbollah's attacks are justifiable as an appropriate retaliation for Israel's actions against Lebanese civilians. Nonetheless, this view is not shared by many in the international community, including in some Muslim countries such as Saudi Arabia, Jordan and Egypt. In the eyes of Hezbollah supporters, tactics such as suicide bombings, assassinations and the kidnapping of foreigners are considered defensible and heroic aspects of the resistance movement against Israel and its allies. This support does not merely derive from the Shiite Muslim community, but has also garnered support from some in Lebanon's non-Muslim community.

Hezbollah takes the view that the creation of the state of Israel is unlawful, that the US and UK are primarily responsible, and that they exacerbate the situation by their support and funding of Israel. Thus, Hezbollah justifies its hostility towards Israel and its allies, seeing any aggression towards Israel as a patriotic resistance to oppression. Notable examples of such hostility include the 1983 US Embassy Bombing in Beirut, the hijack of TWA Flight 847 in 1985 and the 1992 Israeli Embassy attack in Buenos Aires.

Hezbollah claims that its main source of income comes from zakat, or paying alms to the poor. Zakat is one of the five pillars of Islam, and every Muslim must give 2.5% of their wealth, if it is in excess of an annual limit, to those who can receive alms (8 categories of people qualify). These funds are said to be supplemented by donations from Muslims around the world, including charities. Donations are usually collected during gatherings organised by expatriates in these countries, with the funds subsequently remitted to associated organisations and ultimately to Hezbollah. It is claimed that Hezbollah also uses charities and front organisations to conceal its fundraising activities.

A further allegation made by researchers is that Hezbollah allegedly receives substantial funding from Iran, with some analysts estimating that the revenue from this source reaches around US\$200m a year. Syria is also alleged to provide logistical support in the form of banking and other trading avenues. Finally, Hezbollah is apparently heavily supported by wealthy Shiites, some of whose contributions are legally dubious, with several donors being investigated and indicted by enforcement authorities for criminal activities, such as counterfeiting, trading conflict diamonds, and distributing illegal narcotics and pirated software. Conflict diamonds are thought to have provided Hezbollah with a method of transferring money, converting cash into these small and easily transportable commodities. The US Treasury Department has also accused Hezbollah of counterfeiting US currency. The legitimacy of Hezbollah funds therefore remains highly questionable.

While the US has had some success in disrupting the funding of Hezbollah, for example through actions taken against Iranian banks like Bank Saderat and Bank Sepah, ex OFAC Director Adam Szubin has stated in Congressional Testimony that: "one cannot hope to apply effective financial pressure against a group like Hezbollah so long as it maintains massive inflows from a state sponsor of terrorism, in this case the Iranian government."

Today Hezbollah can be considered an organisation of international reach. Its theatre of operations includes Europe, North and South America, East Asia, and other parts of the Middle East. It is also a player in Lebanon's mainstream political arena, holding 11 of 30 cabinet seats within the Lebanese government since a national unity government was established in 2008, as well as broadcasting its own radio and satellite television stations.

As recently as 30 January 2013 Hezbollah has returned to centre-stage in the political relations of the Middle East following an Israeli air strike on a convoy believed to be transporting anti-aircraft weapons from Syria to Hezbollah.

Iraq



The region of Iraq was historically known as Mesopotamia (Greek: "between the rivers") and home to the world's first known civilization, the Sumerian culture, followed by the Akkadian, Babylonian, and Assyrian cultures, whose influence extended into neighboring regions as early as 5000

BC and are often considered as the "Cradle of Civilization". Whilst the region was conquered from both West (Alexander the Great) and East (the Parthians), the Mongols it was the Ottomans who took Baghdad from the Persians, until the loss of their empire at the end of the first world war. The British were given the mandate for the region, initially combining two regions, Baghdad, and Basra into a single country in 1921 and in 1926, adding Mosul in the north, forming the territorial boundaries of the modern Iraqi state.

Britain granted independence to Iraq in 1932, under the rule of King Faisal, a Hashemite king. The Hashemite Kings would rule with selected Sunni support until a military coup in 1958 toppled the regime. Whilst the new military looked to the Soviet Union for support, the regime was itself toppled in another coup in 1968 this time by the Arab Socialist Baath Party. This movement eventually gradually came under the control of Saddam Hussein in 1979 who assumed the Presidency, leading to 25 years of calamitous rule, including the Iran Iraq war, use of chemical weapons, major abuses against kurdish and shia in Iraq, the invasion of Kuwait, the bombing of Israel, the ejection from Kuwait, the supporting of terrorism and his weapons of mass destruction programmes being the most notable ending in his downfall following the US led invasion in 2003. In December, 2006 after being found and tried he was hanged and killed, a fate which would come to many of his closest supporters. The power vacuum and the violence that predates the fall of Saddam Hussein, led to bloodletting and many atrocities, including a violent insurgency, that included not only local actors but also regional and international ones. Immediately Al-Qaeda took advantage of the insurgency to entrench itself in the country concurrently with an Arab-Sunni led insurgency and sectarian violence, establishing its affiliate Al-Qaeda in the land of the two rivers or AQ in Iraq, which produced splinter groups including the Abdullah Azzad Shaheed Brigades and other Sunni and Kurdish insurgency groups such as Jaish Ansar al-Sunna and Ansar al-Islam and in response Shia groups such as Khata'ib Hezbollah. In 2005, more than 63% of eligible Iraqis came out across the country with 78% voting in favour a new constitution. The new constitution had overwhelming backing among the Shia and

Kurdish communities, but was overwhelmingly rejected by Arab Sunnis. Under the terms of the constitution, the country conducted fresh nationwide parliamentary elections on December 15 to elect a new government. The overwhelming majority of all three major ethnic groups in Iraq voted along ethnic lines, turning this vote into more of an ethnic census than a competitive election. Iraq continues to be divided largely on ethnic lines, with Iraqi politicians and civilians alike under significant threat by the various factions that continue to promote violence as a political weapon. The ongoing violence in Iraq has been incited by an amalgam of religious extremists that believe an Islamic Caliphate should rule, old sectarian regime members that had ruled under Saddam that want back the power they had, and Iraqi nationalists and Kurdish separatists.

Before the fall of Saddam Hussein in 2003, the Ba'ath Party officially ruled as a Sunni minority. The current Prime Minister of Iraq is Nouri al-Maliki, who heads a government that is mainly supported by the majority Shia populace. Maliki was re-elected in 2010. It has been estimated that the number of deaths caused as a result of the Iraq war and its bloody aftermath, are at least 100,000 with other estimates putting the figure as high as half a million. Terrorists are active in Iraq, being placed 3rd by Maplecroft of at risk countries for the likelihood of a terrorist attack ahead of Afghanistan and South Sudan and before Somalia and Pakistan. According to the Global Terrorism Database of terrorist fatalities and incidents since 1970 Iraq tops the list with 17,754 ahead of Sri Lanka and India and Iraq is also the 7th most attacked Country by terrorists. For more details see Part 1 Section 1 Terrorism Finance above.

Iraq's economy is primarily cash-based and whilst narcotics trafficking and narcotics-based money laundering are not major problems, smuggling is endemic, often involving consumer goods, cigarettes, and petroleum products. Bulk cash smuggling, trafficking in persons, and intellectual property rights violations are also concerns. Ransoms from kidnappings and extortion are often used to finance terrorist and criminal networks. Credible reports of counterfeiting exist. Trade-based money laundering, customs fraud, and other forms of value transfer allow criminal organisations the opportunity to earn, move and store supporting funds and illicit proceeds under the guise of legitimate trade. Hawala networks, both licensed and unlicensed, are widely used for legitimate as well as illicit purposes. Corruption is also a major challenge.

According to Transparency International in 2013, Iraq's is the most corrupt government in the Middle East with a rating of 171 out of 175. The 2011 report "Costs of War" from Brown University's Watson Institute for International Studies concluded that U.S. military presence in Iraq has not been able to prevent this corruption, noting that as early as 2006, "there were clear signs that post-Saddam Iraq was not going to be the linchpin for a new democratic Middle East."

Special Focus 6

Al-Qaeda Organisation in the Land of the Two Rivers / Al-Qaeda in Iraq



Tanzim Qa'idat al-Jihad Fi Bilad al-Rafidayn is the current name of the terrorist group Jama'at al-Tawhid Wa'al-Jihad, formerly led by Abu Musab Zarqawi. The US State Department has understood this new name, which is translated as the Al-Qaeda Organisation in the Land of the

Two Rivers, to imply that Zarqawi saw his group as the centre of Jihadist activities in Iraq. This change was made after Zarqawi formally pledged his alliance to Al-Qaeda in a letter addressed to Osama bin Laden recovered by Coalition forces in 2004.¹²

Despite the change in name, the letter makes it clear that the goals of Zarqawi's group, to overthrow the interim Iraqi government and establish an Islamic state in Iraq by forcing out the US-led coalition, remain constant. AQI is believed to be comprised of foreign terrorists, elements of the Kurdish Islamist group Ansar al-Islam, and indigenous Sunni Iraqis.

The group issues claims of responsibility regularly in Iraq for attacks on American and Iraqi security forces, often claiming several attacks in one day. The AQI uses a variety of tactics that include RPG attacks against armoured vehicles, guerrilla style attacks by armed militants, suicide bombings, and the kidnapping and beheadings of foreigners.

A video released in May 2004 gained notoriety for depicting Zarqawi brutally beheading Nicholas Berg, an American civilian contractor in Iraq. However, the group has increasingly eschewed such tactics since Zarqawi swore allegiance with Al-Qaeda. Instead, AQI, which is believed to derive most of its domestic support from Sunni Arabs, targets (in order of priority) Shiite Arabs, who are seen as pro-American betrayers of the true faith, Coalition forces and their local support, including the Iraqi security forces, and Kurds, who are perceived to act as a "Trojan Horse" for Jewish economic infiltration into Iraq.

In addition to frequent smaller scale attacks in Iraq, the group claimed responsibility for the bombing of three hotels in Amman, Jordan that left 67 people dead and injured more than 150. A stern rebuke issued by Al-

Qaeda number two, Ayman al-Zawahiri, shortly after the attack seems to have stopped the selection of targets outside of Iraq.

Zarqawi's letter to bin Laden revealed many problems that the former believed AQI would face in the coming years. The Sunni insurgent leader pointed out that as American forces are drawn down or removed from the front lines and indigenous Iraqi forces take their place, attacks perpetrated against security forces will increasingly be seen as anti-Iraqi attacks, rather than anti-occupation ones. Zarqawi confessed that his fighters' freedom of movement had become increasingly restricted and that the "future has become frightening".

According to Zarqawi the local Sunni Iraqi resistance was inexperienced and unwilling to sacrifice for the cause, whereas battle-tested foreign Mujahideen were too small in number to affect significant change. Zarqawi went on to complain that the Sunni Iraqi masses have "no firm principles" and that "their religion is mercurial". Additionally, the letter illuminated a strategic plan for victory, despite these odds. Importantly, Zarqawi highlighted the importance of the information warfare campaign, stating that the "pen and the sword complement each other". He targeted the Shia as the main enemy, hoping to incite sectarian strife and thus provoke the Sunni "silent majority" into armed action in the ultimate battle for the future of Islam.

In a speech broadcast over the internet on 23 January 2005, Zarqawi denounced the upcoming Iraqi elections, calling candidates "demi-idols" and voters "infidels." Zarqawi's statement, declaring a "fierce war" against democracy, accused the Americans of rigging the election in favour of Iraq's Shi'ite population. Increased Sunni Arab participation in Iraq's December 2005 parliamentary elections offered hope to some that support for wider insurgency may be abating. However, violence resumed following a lull in attacks during the election, including attacks by AQI. In January 2006, the group was one of six insurgent organisations to unify under the Mujahideen Shura Council. For a time all attacks perpetrated by AQI were claimed in the name of the Council. Zarqawi himself was killed in a US air strike in June 2006, and until 2010 his successor as head of operations in Iraq was Abu Ayub al-Masri. In October of 2006 al-Masri openly expressed his intention to establish a new caliphate in the region by declaring the 'Islamic State of Iraq' and began to use this as the pseudonym under which to claim attacks perpetrated by AQI. In 2010 al-Masri, along with fellow senior leader al-Baghdadi, were killed in a raid and subsequently replaced by Abu Baker al-Baghdadi al-Husseini al-Qurashi and Abu Ibrahim al-Issawi as the organisation's leaders. The months between March and May of 2010 represented a period in which the organisation suffered considerable losses, with Iraqi and US security forces capturing or killing 34 of 42 senior leaders.

In the years following 2010 AQI has continued to use

violent strikes in an attempt to incite large-scale sectarian violence, however this is an end in which it has been largely unsuccessful. Rather Sunni leaders have agreed to participate in the political process alongside Shi'ite Muslims, and two democratic elections have taken place. Nonetheless the organisation has not dwindled into obscurity, in 2011 it was estimated that the group had between 1000 and 2000 members. While the majority of its attacks are conducted in Iraq, AQI has also undertaken operations in neighbouring Jordan.

More recently the organisation has expanded to join the fight in neighbouring Syria, under the umbrella group known as The Islamic State of Iraq and Syria (ISIS) also known as The Islamic State of Iraq and the Levant.

Abdullah Azzam Shaeed Brigades - Iraq

The Abdullah Azzam Brigades was formed as an off-shoot of AQI in 2009 with local networks in countries across the Middle East, mostly in the Levant area including Jordan, and is named after Sheikh Abdullah Azzam, a Palestinian from Jordan who was among the first arabs to volunteer to join the Afghan Jihad. The Lebanese branch is called the Ziad al-Jarrahd Battalion.

Ansar al-Islam (AI)/AQ Kurdish Battallions - Iraq

Ansar al-Islam was designated as a US Foreign Terrorist Organisation on 22 March 2004, Ansar al-Islam's goals include expelling the western interests from Iraq and establishing an independent Iraqi state based on Sharia law. AI was established in 2001 in Iraqi Kurdistan with the merger of two Kurdish extremist factions that traced their roots to the Islamic Movement of Kurdistan. On May 4, 2010 Abu Abdullah al-Shafi'i, Ansar al-Islam's leader was captured by US forces in Baghdad and remains in prison. On 15 December 2011 AI announced a new leader, Sheikh Abu Hashim Muhammad bin Abdul Rahman al Ibrahim. AI is now thought to be known as AQ Kurdish Battallions.

AI has conducted attacks against a wide range of targets including the Iraqi government and security forces, and US and Coalition forces. AI has conducted numerous kidnappings, executions, and assassinations of Iraqi citizens and politicians. The group has either claimed responsibility or is believed to be responsible for attacks in 2011 that killed 24 and wounded 147 people. On February 7, AI posted leaflets in Kirkuk warning of an attack on a Kurdish militia in retaliation for the arrest of Muslim women in the city. Two days later, a series of car bombs exploded in Kirkuk, destroying the militia's headquarters and injuring two nearby police patrols. The attack killed ten and wounded 90. On 13 October, 16 civilians and two police officers were killed and 43 others wounded in a double improvised explosive device attack in Baghdad. The group was also responsible for kidnappings in February and December 2011 and more recently.

Jamaat Ansar al-Sunna - Iraq

Formerly Jaish Ansar al-Sunna, this group whose name means "Assembly of the Helpers of Sunnah" is one of the many Iraqi Sunni insurgent groups that is battling the forces of the Shia led Nouri al-Maliki government. The group adheres to mainstream Wahabbism. The group is based in northern and central Iraq, and includes mostly Iraqi (both Sunni Arab and Sunni Kurdish) fighters. The group was founded in September 2003 as an umbrella organisation for guerrillas, with former members of Ansar al-Islam, with members currently residing in Iran after a 2003 joint operation by Iraqi and US forces forced them to flee Iraq. Ansar al-Sunna is thought to have had links with organisations operating in Iraq including, the formerly Abu Musab al-Zarqawi backed, Jama'at al-Tawhid wal-Jihad (Al-Qaeda in Iraq), though has since, with others engaged in violent conduct against AQ in Iraq. In 2007 representatives of the Ansar al-Sunna were instrumental in forming an alliance of Sunni militant groups to prepare for the withdrawal of American and allied forces. The new alliance is composed of seven groupings explicitly excluding Al-Qaeda and the Baath-party. Ansar al-Sunna has claimed responsibility for suicide bombings and kidnap and beheadings in Iraq, including the devastating attacks on the offices of two main Kurdish political parties, KDP and PUK, in Irbil in 2004, that killed at least 109 people.

Khata'ib Hezbollah (KM) - Iraq

Khata'ib Hezbollah was formed in 2006 and is a radical Shia Islamist group with an anti-Western outlook and extremist ideology that has conducted attacks against Iraqi, US, and Coalition targets in Iraq. KH has threatened the lives of Iraqi politicians and civilians that support the legitimate political process in Iraq. The group is notable for its extensive use of media operations and propaganda by filming and releasing videos of attacks. KH has ideological ties to Lebanese Hezbollah and may have received support from that group and its sponsor, Iran. KH has been responsible for numerous violent terrorist attacks since 2007, including improvised explosive device bombings, rocket propelled grenade attacks, and sniper operations. In 2007, KH gained notoriety with attacks on US and Coalition Forces in Iraq. KH was particularly active in the summer of 2008, recording and distributing video footage of its attacks against US and Coalition soldiers. Using the alias "Hezbollah Brigades in Iraq," KH filmed attacks on US Stryker vehicles, Abrams tanks, and Bradley armored personnel carriers. In 2009, KH continued to release videos of attacks ranging in date from 2006 to 2008 on the Internet. In June 2011, five US soldiers were killed in a rocket attack in Baghdad, Iraq, when KH assailants fired between three and five rockets at the US military base Camp Victory, which surrounds Baghdad's International airport. KH is almost entirely dependent on support from Iran and Lebanese Hezbollah. Khata'ib Hezbollah was designated as a US Foreign Terrorist Organisation on 2 July 2009.

Iran



Around 2000 B.C. the Parsua tribe (from which the Persians derive their name) left central Asia in search of greener pastures for their cattle, eventually settling near what is now the Persian Gulf. By around 545 B.C. they had the largest empire on Earth, stretching 3000 miles across to and

including Asia Minor (now Turkey) and ruled over by Cyrus the Great.

Whilst conquering Greece had already been attempted, Xerxes I, in 480 BC tried again. He amassed a great army of hundreds of thousands of warriors, which was one of the largest armies assembled during ancient times. Xerxes initially won the Battle of Thermopylae against much smaller army from Sparta; however, the Greek fleet defeated his navy at the Battle of Salamis and he was eventually forced to retreat. Many historians believe that a Persian victory would have seriously altered World history, negatively affecting the development of Ancient Greece, and by extension western civilization, and this has led to claims that Salamis was one of the most significant battles of all times. Notwithstanding this defeat, the Persian Empire continued to dominate the area until around 334 B.C. when they were conquered by the Macedonian general Alexander The Great.

In succeeding centuries, Persia was invaded by the Parthians, the Arabs, the Mongols and various Turkish dynasties. After the Arab conquest in the middle of the 7th century, Islam became the dominant religion, and as a result of rule by one of the Turkish dynasties in the 16th Century, the Shiite branch of Islam became the official religion on Persia. The Persians fought against the Ottomans and once more established themselves as a major power. After the first World War in 1921, Reza Khan Pahlavi an army officer, established a military dictatorship and made himself a hereditary Shah, and ruler of a country that had recently discovered oil. He was followed after the second world war by his son Mohammad Reza Pahlavi. The new Shah introduced the White Revolution, a series of economic, social and political reforms with the proclaimed intention of transforming Iran into a global power and modernizing the nation by nationalizing certain industries and granting women suffrage.

In response, conservative clerical forces led by Ayatollah Khomeini in 1963 revolted and opposed the Shah. Whilst Khomeini and the Islamists would be put down at this time they would succeed later in 1979 when the Shah was forced into exile and following the Iranian

Revolution, clerical forces led by Ayatollah Khomeini, established a theocratic system of government with ultimate political authority vested in a learned religious scholar referred to commonly as the Supreme Leader who, today is Khomeini's successor, namely, Ayatollah Khamenei.

US-Iranian relations became strained when a group of Iranian students seized the US Embassy in Tehran in 1979 and held embassy personnel hostages until early 1981. The US cut off diplomatic relations with Iran in 1980. During the period 1980-88, Iran fought a bloody, indecisive war with Iraq.

Iran has been designated by the US as a state sponsor of terrorism for its activities in Lebanon and elsewhere in the world and remains subject to US, UN, and EU economic sanctions and export controls because of its continued involvement in terrorism and its nuclear weapons ambitions.

In 1984, the US designated Iran as a state sponsor of terror, due to its continued support to multiple terrorist organisations, including Hezbollah and the Palestinian Islamic Jihad (PIJ). In 2011, the U.S. Government identified Iran as a state of primary money laundering concern and in 2012, the FATF urged jurisdictions around the world to impose countermeasures to protect their financial sectors from illicit finance emanating from Iran. Iran is known to use its state-owned banks to channel funds to terrorist organisations and finance its nuclear and ballistic missile programmes.

The US has designated at least 20 Iranian banks and subsidiaries under counter-proliferation and terrorism authorities. Iran is subject to US, UN, and EU economic sanctions and export controls because of its continued involvement in terrorism and its nuclear weapons ambitions. Iran is a presumed source, transit, and destination country for men, women, and children subjected to sex trafficking and forced labour.

In a move that may enable reformers to come to the fore and after eight acrimonious years under former President Ahmadinejad, 2013 elections saw the moderate cleric Hassan Rouhani gain power.

Rouhani, a PhD graduate from Glasgow Caledonian University and a former nuclear negotiator, has pledged to find a way out of the current stalemate over Iran's nuclear programme, and to have lifted international sanctions against the country.

Nevertheless hardliners remain in control of key aspects of Iran's political system, not least the continued leadership of the country by the Supreme leader Ayatollah Khomeini.

Despite substantial interdiction efforts and considerable control measures along the border with Afghanistan, Iran remains one of the primary transshipment routes

for Southwest Asian heroin to Europe and as a result suffers one of the highest opiate addiction rates in the world, and has an increasing problem with synthetic drugs. Iran's merchant community makes active use of money and value transfer systems, including hawala and moneylenders. Many hawaladars and traditional bazaaris are linked directly to the regional hawala hub in Dubai. Over 300,000 Iranians reside in Dubai, with more than 8,000 Iranian-owned companies based there. Iran is ranked 133 out of 174 countries listed in Transparency International's 2012 Corruption Perception Index. There is pervasive corruption within the ruling and religious elite, government ministries, and government-controlled business enterprises.

Islamic Revolutionary Guards Corps - Iran

The Islamic Revolutionary Guard Corps (IRGC) was formed by late supreme leader Ayatollah Khomeini in the wake of the 1979 Islamic Revolution that ousted Shah Reza Pahlavi. The country's premier security institution of more than 100,000 strong, the IRGC is charged with defending the Islamic Republic against internal and external threats. The IRGC fields an army, navy, and air force, while managing Iran's ballistic missile arsenal and irregular warfare operations through its elite Quds Force. The Quds Force has supported terrorist activities and armed pro-Iranian militant groups across the Middle-East and beyond, including in Lebanon, most notably Hezbollah, the Palestinian territories, Iraq, Afghanistan, the Gulf states, and elsewhere including most recently providing weapons and other material support to help President Bashar al-Assad suppress the uprising in Syria.

The Guards also control Iran's Basij Resistance Force, an all-volunteer paramilitary wing, which consists of as many as one million conscripts. Whilst the IRGC have political and military authority, they also have a significant financial clout, including control of a number of Bonyads. The Los Angeles Times estimated in 2007 that the group, which was tasked with rebuilding the country after the Iran-Iraq war, now has ties to more than one hundred companies that control roughly US\$12bio in construction and engineering capital. Critical to the success of the IRGC in providing sufficient funding sources are Iranian Bonyads which make up to approximately 30% of Iran's GDP. Bonyads are tax-exempt charitable entities. Comprising well over 120 semi-state tax-exempt monetary foundations, Bonyads have been in existence for a long time. Founded as royal foundations by the Shah the original Bonyads were criticised for providing a "smokescreen of charity" to patronage, economic control, for-profit wheeling and dealing done with the goal of "keep[ing] the Shah in Power."

After the 1979 revolution, the Bonyads were nationalized and the assets of many Iranians whose ideas or social positions ran contrary to the new Islamic government were also confiscated and given to the Bonyads. The largest of today's Bonyads is likely the "Foundation of the Oppressed and Disabled," which is the

principal holder of assets seized from the Shah and is sometimes referred to as the "government within the government." This Bonyad has been run by hardliners and former officials of the IRGC. In 1982, the foundation owned 203 manufacturing and industrial factories, 472 large farms, 101 construction firms, and 238 trade and service companies. In the past two decades it has used these already large assets to expand its activities into all areas of the economy, including manufacturing, commerce, banking, tourism, and telecommunications. This Bonyad is long suspected also of being involved in procuring weapons of mass destruction (WMD) as well as the illegal importation of alcohol.

Mujahadin-e Khalq (MEK) - Iran

The Mujahadin-E Khalq Organisation (MEK) is a Marxist-Islamic Organisation that seeks the overthrow of the Iranian regime through its military wing, the National Liberation Army (NLA), and its political front, the National Council of Resistance of Iran (NCRI). The MEK was founded in 1963 by college-educated Iranian Marxists who opposed the country's pro-western ruler, Shah Reza Pahlavi. The group participated in the 1979 Islamic Revolution that replaced the Shah with a Shiite Islamist regime led by Ayatollah Khomeini. However, the MEK's ideology, a blend of Marxism, feminism, and Islamism, was at odds with the post-revolutionary government, and its leadership was soon executed by the Khomeini regime. In 1981, the group resettled in Paris, where it began supporting Iraq in its eight-year war against Khomeini's Iran. In 1986, after France recognised the Iranian regime, the MEK moved its headquarters to Iraq, which facilitated its terrorist activities in Iran. From 2003 through the end of 2011, roughly 3,400 MEK members were encamped at Ashraf in Iraq. Before Operation Iraqi Freedom began in 2003, the MEK received all of its military assistance and most of its financial support from Saddam Hussein, and since the MEK increasingly has to rely on front organisations to solicit contributions from expatriate Iranian communities.

Jundallah - Iran/Baluchestan

Since its 2003 inception, Jundallah, a violent extremist organisation that operates primarily in the province of Balochistan of Iran, as well as the greater Baluchestan area of Afghanistan has engaged in numerous attacks and killings of Iranian civilians and government officials. Jundallah wants to secure recognition of Baluchi rights from Iran and to spread awareness of the Baluchi situation through violent and non-violent means. A 2009 suicide bomb attack in a marketplace in Pishin in the Sistan and Baluchestan Province killed more than 40 people, was reportedly the deadliest terrorist attack in Iran since the 1980s. In 2010 a suicide bomb attack inside the Imam Hussein Mosque in Chabahar killed an estimated 35 to 40 civilians and wounded 60 to 100. In July 2010, Jundallah attacked the Grand Mosque in Zahedan, killing approximately 30 and injuring an estimated 300.

Gulf States



The Gulf States are those Arab states bordering the Persian Gulf, being Kuwait, Bahrain, Oman, Qatar, Saudi Arabia and United Arab Emirates, all part of the Gulf Cooperation Council. All of these Arab states have significant revenues from oil and gas and, with the exception of Saudi Arabia,

have small local populations. Other states also border the Gulf including Iran and Iraq though these are less described as Gulf States and more regional powers within the wider middle east. The Gulf States, and their ruling families are predominantly Sunni Islamic, with Bahrain, the one outlier with the majority being Shiite versus the minority Sunni, though with a Sunni ruling family. Whilst other Bordering nations Iraq and Iran are not considered pure Gulf States, both are Shia Islamic dominated, though under Saddam Hussein the Sunni minority ruled. Conversely in Syria, the ruling class under President Bashar al-Assad are the Alawites a sect which is an offshoot religion of Shiite Islam, in a majority-Sunni country. Whilst Iran supports much of the Shia in the region, the Sunnis are supported by the Gulf States and on this axis much can be explained. For example, the rebels trying to topple Bashir al-Assad are receiving military and political support from majority-Sunni Saudi Arabia, UAE, Kuwait, Bahrain and Qatar.

This rivalry between Shia and Sunni, in particular between the main regional powers Iran and Saudi Arabia has even spread to the naming of the Gulf region itself. For Centuries the name of the gulf, has been known as the Persian Gulf after the land of Persia (Iran), but is since the 1960s, being challenged by the naming of the area as the Arabian Gulf. Whatever the name it is a very important waterway, especially one that is necessary to ensure the continued flow from the region of Oil.

United Arab Emirates

The United Arab Emirates (UAE) is situated in the Southeast of the Arabian Peninsula, bordering Oman and Saudi Arabia. In December 1971, the UAE became a federation of six emirates, Abu Dhabi, Dubai, Sharjah, Ajman, Umm al-Quwain, and Fujairah, while the emirate of Ras Al Khaimah joined the federation in 1972. The capital city is Abu Dhabi, located in the largest and wealthiest of the seven emirates.

Since its Federation in 1971, the UAE has developed rapidly and is now noted for its modern infrastructure, international events and status as a trade and transport

hub. The President of the UAE is His Highness (HH) Sheikh Khalifa bin Zayed Al-Nahyan, who is also Ruler of Abu Dhabi Emirate. The Ruler of Dubai Emirate, HH Sheikh Mohammed bin Rashid Al-Maktoum, is the Vice-President, Prime Minister and Defence Minister. The UAE is the Middle East's second largest economy after Saudi Arabia and one of the wealthiest countries in the region on a per capita basis.

A significant portion of the money laundering activity in the UAE is likely related to proceeds from illegal narcotics produced in South West Asia. Narcotics traffickers from Afghanistan, where most of the world's opium is produced, are increasingly reported to be attracted to the UAE's financial and trade centers. Domestic public corruption contributes little to money laundering or terrorist financing. Regional hawalas and associated trading companies in various expatriate communities, most notably the Somalis, have established clearinghouses, the vast majority of which are not registered with the UAE government. Likewise, the UAE's proximity to Somalia has generated reports suggesting some influx and/or transit of funds derived from piracy. There are some indications that trade based money laundering occurs in the UAE and that such activity might support terrorist groups in Afghanistan, Pakistan and Somalia. Other money laundering vulnerabilities in the UAE include exploitation of cash couriers, the real estate sector, and the misuse of the international gold and diamond trade. The Emirates also have an extensive offshore financial center.

Saudi Arabia

The Region of Arabia had been ruled by a patchwork of tribal rulers, for centuries, is the birthplace of Islam and home to Islam's two holiest shrines in Mecca and Medina and was for many centuries under the overall control of the Ottoman Empire. The modern Saudi state was founded in 1932 by Ibn Saud after a 30-year campaign to unify most of the Arabian Peninsula. The conquests which eventually led to the creation of the Kingdom began in 1902 when Ibn Saud captured Riyadh, the ancestral home of his family, the House of Saud, or Al Saud and with British support during World War 1 was able to consolidate Arabia into what is today Saudi Arabia. Ibn Saud received support and formed a long alliance with the followers of 18th Century Imam, Muhammad ibn Abd al-Wahhab, who founded Wahhabism, considered an ultra-conservative branch or sect of Sunni Islam with an aspiration to return to the earliest fundamental Islamic sources of the Quran, without speculative philosophy so as to not transgress beyond the limits of the early Muslims known as the Salaf. The Al Saud regime has been an absolute monarchy since its inception and current King Abdullah is a descendant as is required under the constitution. The king's official title is the Custodian of the Two Holy Mosques, which recognises the importance of religion in Saudi Arabia and to Muslims worldwide. The form of Islam practiced

in Saudi Arabia is influenced by Wahhabism and a result of the early and long lasting alliance between the House of Saud and the followers of Wahhabism. The Wahhabism movement gained unchallenged precedence in the Arabian peninsula through this alliance and with enormous financial support. The Saudi government established the Commission for the Promotion of Virtue and Prevention of Vice, a state religious police unit, to enforce religiously Wahhabi rules of behaviour. Since the 1970s it is estimated that the Saudi government had spent at least US\$87bio propagating Wahhabism abroad, the bulk of this funding going towards the construction and operating expenses of mosques, madrasas and other religious institutions and teachings that preach Wahhabism.

Saudi Arabia is bordered by Jordan and Iraq to the north, Kuwait to the northeast, Qatar, Bahrain and the United Arab Emirates to the east, Oman to the southeast, Yemen in the south, the Red Sea to the west and Persian Gulf to the east. Its population is estimated to consist of 16 million citizens and an additional 9 million registered foreign expatriates and 2 million illegal immigrants. Saudi Arabia has the world's second largest oil reserves and the world's sixth largest natural gas reserves, which account for more than 95% of exports and 70% of government revenue. This has facilitated the transformation of the underdeveloped desert kingdom into one of the world's wealthiest nations, and as one of the 20 most powerful countries in the world. It is considered a regional power, dominating in the Arabian peninsula and competing with Iran and Egypt in the wider Arab Community for leadership status. Saudi Arabia is a growing financial center in the Gulf Region.

With a large expatriate labour community and a predominantly cash-based society, it is susceptible to money laundering and terrorist financing originating from Saudi criminal enterprises, private individuals, and Saudi-based charities. Saudi bulk cash smuggling from individual donor and charities has reportedly been a major source of financing to extremist and terrorist groups over the past 25 years. As one way of addressing the potential diversion of charitable giving, the Saudi government has attempted to consolidate charitable campaigns under Ministry of Interior supervision. With the advent of tighter bank regulations, funds are reportedly collected and illicitly transferred in cash, often via pilgrims performing Hajj or Umrah. Saudi Arabia is a destination country for men and women subjected to forced labour and, to a lesser extent, forced prostitution and men and women from many South And South East Asia Countries voluntarily travel to Saudi Arabia as domestic servants or other low-skilled labourers, but some subsequently face conditions indicative of involuntary servitude. Underground remittance systems such as hawala are also present in Saudi Arabia and have been used to finance terrorism.

Despite serious and effective efforts to counter the funding of terrorism originating from within its borders,

and from branches and offices of entities funded from or controlled Saudi Arabia, for example see Terrorism Financiers in Part 2, Section 7 Cases/Criminals below. Saudi Arabia continues to serve as an important source of funds flowing to Sunni-based extremist groups, through individual sponsored donations from sympathizers and supporters. The major domestic terrorist threat comes from Al-Qaeda in the Arabian Peninsula, with incidents such as the Khobar Towers bombing in 1996, the Riyadh Compound bombings in 2003 and the Khobar Massacre in 2004. Attacks have also been carried out by AQAP in neighboring Yemen also including the bombing of the USS Cole in 2000, which foreshadowed the 2001 attacks on America, carried out by largely Saudi citizens and led by Saudi Citizen Osama bin Laden's Al-Qaeda.

Yemen

North Yemen became independent after defeat of the Ottoman Empire in 1918 after the first World War. In South Yemen, the British only withdrew in 1967. The two countries were formally unified as the Republic of Yemen in 1990. A brief civil war in 1994 and fighting in 2004 between the government and rebels seeking a return to traditional Islam ended in early 2010 with a ceasefire that continues to hold. Public rallies starting in January 2011 in the capital Sana'a against then President Salih inspired by similar demonstrations in Tunisia and Egypt, as part of the so called Arab Spring. These led, by November 2011, to Salih stepping down and transferring his powers to Vice President Abd Rabuh Mansur Hadi, who stood for and won subsequent elections in 2012. Government corruption, a largely cash-based economy and lax government enforcement of existing laws and regulations render Yemen vulnerable to money laundering and other financial abuses, including possible terrorist financing. Yemen has a large underground economy due, in part, to the profitability of the smuggling of trade goods and contraband. Criminal proceeds in Yemen tend to emanate from foreign criminal activity, including smuggling by criminal networks, and, possibly, terrorist groups, including Al-Qaeda in the Arabian Peninsula. There is also evidence that khat is smuggled from Yemen as well as from East Africa into Western Europe and the US with profits laundered and repatriated via hawala networks.

Transparency International lists Yemen as 167 out of 175 on its 2013 Corruption Perception Index. Yemen is included in the October 2012 Financial Action Task Force (FATF) Public Statement because it has not made sufficient progress in implementing its action plan and continues to have certain strategic anti-money laundering/counter-terrorist financing deficiencies, including the inadequate criminalization of money laundering and terrorist financing, the inability to freeze terrorist assets, and the lack of capacity of supervisory entities and the financial intelligence unit.

Special Focus 7

Al-Qaeda in the Arabian Peninsula - Saudi/Yemen



Al-Qaeda in the Arabian Peninsula (AQAP) is a militant Islamist organisation, primarily active in Yemen and Saudi Arabia, and acts as an affiliate of Al-Qaeda. Like Al-Qaeda, it opposes the Al Saud monarchy. AQAP was formed in January 2009 from a merger of al-Qaeda's Yemeni and Saudi branches.

The Saudi group had been effectively suppressed by the Saudi government, forcing its members to seek sanctuary in Yemen. It is believed to have several hundred members. Osama bin Laden was a Saudi citizen whose father was born in Yemen. It is considered the most active of Al-Qaeda's branches, or "franchises," that emerged due to weakening central leadership.

According to US counter-terrorism officials, Anwar al-Awlaki¹² was the main force behind AQAP's decision to transform itself from a regional threat into Al-Qaeda's most active affiliate outside Pakistan and Afghanistan. The percentage of terrorist plots in the West that originated from Pakistan declined considerably from most of them (at the outset), to 75% in 2007, and to 50% in 2010, as Al-Qaeda shifted to Somalia and Yemen.

US Secretary of State Hillary Clinton formally designated AQAP a terrorist organisation on December 14, 2009. On August 25, 2010, The Washington Post said the CIA believed Yemen's branch of Al-Qaeda had surpassed its parent organisation, Osama bin Laden's core group, as a threat to the US homeland.¹³

AQAP was responsible for the USS Cole bombing in October 2000 in the southern port of Aden, killing 17 US sailors. The Aden-Yemeni Islamic Army was also believed to have been involved in this attack. In 2002, an AQAP attack damaged a French supertanker in the Gulf of Aden. The Global Terrorism Database attributes the 2004 Khobar massacre also to the group. An attack in 2008 on the US Embassy in Yemen killed 19 and was claimed by an AQ affiliate, the Islamic Jihad of Yemen. Abdulhakim Mujahid Muhammad, formerly known as Carlos Leon Bledsoe, a Muslim convert who had spent time in Yemen, opened fire in 2009 with an assault rifle in a drive-by shooting on soldiers in front of a US military recruiting office in Little Rock, Arkansas, US in a jihad attack. He killed Private William Long, and wounded Private Quinton Ezeagwula. He said that he was affiliated with and had been sent by AQAP.

In August 2009, an AQAP suicide bomber tried to kill Prince Mohammed bin Nayef, who heads Saudi Arabia's anti-terrorism campaign and is a member of the Saudi royal family. In 2009, AQAP also carried out a suicide attack in Yemen that killed four South Korean tourists. AQAP said it was responsible for attempted bombing on North West Airlines Flight 253 as it approached Detroit on 25 December 2009. In that incident, Umar Farouk Abdulmutallab reportedly tried to set off plastic explosives sewn to his underwear, but failed to detonate them properly.

On February 8, 2010, deputy leader Said Ali al-Shihri called for a regional holy war and blockade of the Red Sea to prevent shipments to Israel. In an audiotape he called upon Somalia's al-Shabaab militant group for assistance in the blockade. The 2010 cargo plane bomb plot was discovered on October 29, 2010, when two explosive-laden packages bound for the US via cargo planes were found, based on intelligence received from government intelligence agencies, in the UK and the United Arab Emirates.

In November 2010 the group announced a strategy, called "Operation Hemorrhage", that it said was designed to capitalize on the "security phobia that is sweeping America." The programme would call for a large number of inexpensive, small-scale attacks against US interests with the intent of weakening the US economy.

On 21 May 2012, a soldier wearing a belt of explosives carried out a suicide attack on military personnel preparing for a parade rehearsal for Yemen's Unity Day. With over 120 people dead and 200 more injured, the attack was the deadliest in Yemeni history. AQAP claimed responsibility for the attack.

During the June 2012 Al-Qaeda retreat from key southern Yemeni stronghold, the organisation planted land mines, which killed 73 civilians. According to the governor's office in Abyan province, 3,000 mines were removed from around Zinbar and Jaar. Also in 2012 a funeral service was attacked in Yemen killing 45.

Ansar al-Sharia - Yemen

In the wake of the 2011 Yemeni revolution, an Islamist insurgent organisation called Ansar al-Sharia (supporters of Islamic Law), emerged in Yemen and began to seize control of areas in the Abyan Governorate and surrounding areas and declaring them an Islamic emirate. There was heavy fighting with the Yemeni security forces over the control of these territories, with Ansar al-Sharia driven out of most of their territory over 2012. In October 2012, the UN and the US designated Ansar al-Sharia (Yemen) as an alias for AQAP. The State Department described the establishment of Ansar al-Sharia (Yemen) as an attempt to attract followers in areas of Yemen where AQAP had been able to establish territorial control and implement its interpretation of Sharia.

Egypt



Egypt is a country spanning the northeast corner of Africa and southwest corner of Asia across the Sinai Peninsula. Most of its territory lies within North Africa and is bordered by the Mediterranean Sea to the north, the Gaza Strip and Israel to the northeast, the Gulf of Aqaba to the east,

the Red Sea to the east and south, Sudan to the south and Libya to the west. Egypt is the 15th most populated country in the world, with the great majority of its over 84 million people living near the banks of the Nile River. The English name Egypt is derived from the ancient Greek Agyptos via Middle French Egypte and Latin Aegyptus.

Egypt has one of the longest histories of any modern state, having been continuously inhabited since the 10th millennium BC. A unified kingdom arose circa 3200 B.C., and a series of dynasties ruled in Egypt for the next three millennia. The last native dynasty fell to the Persians in 341 B.C., who in turn were replaced by the Greeks, Romans, and Byzantines. It was the Arabs who introduced Islam and the Arabic language in the 7th century and who ruled for the next six centuries. A local military caste, the Mamluks took control about 1250 and continued to govern after the conquest of Egypt by the Ottoman Turks in 1517. Completion of the Suez Canal in 1869 elevated Egypt as an important world transportation hub. Ostensibly to protect its investments, Britain seized control of Egypt's government in 1882, but nominal allegiance to the Ottoman Empire continued until 1914. Partially independent from the UK in 1922, Egypt acquired full sovereignty from Britain in 1952. Egypt united with Syria in 1958 under nationalist leader Gamal Nasser but this lasted only until 1961.

A rapidly growing population (the largest in the Arab world), limited arable land, and dependence on the Nile all continue to overtax resources and stress society. The government has struggled to meet the demands of Egypt's population through economic reform and massive investment in communications and physical infrastructure. Inspired by the 2010 Tunisian revolution, Egyptian opposition groups led demonstrations and labour strikes countrywide, culminating in President Hosni Mubarak's ouster. Egypt's military assumed national leadership until a new parliament was in place in early 2012. That same year, Mohammed Mursi representing the Muslim Brotherhood won the Presidential election and a new constitution was affirmed. In July 2013, the military ousted Mursi and he was replaced by interim President Adly Mansour.

Muslim Brotherhood - Egypt

A widespread Islamist organisation founded in 1928 in Egypt, the Brotherhood seeks to Islamise societies from the ground up and compel governments in Muslim countries to adhere to sharia, or Islamic law. At various times in its history, the group has used or supported violence and has been repeatedly banned in Egypt for attempting to overthrow the government. Since the 1970s, however, the Egyptian Brotherhood disavowed violence and sought to participate in Egyptian politics, finally coming to power following the recent Egyptian revolution that flowed from the Arab Spring, but also being ousted by the Egyptian Army supported by much of the population following a partisan and unpopular Presidency. The US and European governments do not include the group on its list of terrorist organisations, although Russia does. There are new calls to include the Brotherhood due to its response to its ousting, though the politics and actions of the Army and their response is still being debated. In the past, whilst the Brotherhood maintained its non-violent approach, and built a network of branches in over 70 countries, some terrorist groups—including Hamas, Jamaat al-Islamiyya, and Al-Qaeda—have historic and ideological affiliations with the Brotherhood. In addition, some of the world's most dangerous terrorists were once Egyptian Muslim Brotherhood members, including Osama bin Laden's deputy and now head of AQ al-Zawahiri.

Egyptian Islamic Jihad (EIJ) - Egypt

The Egyptian Islamic Jihad is a terrorist organisation that has been active since the late 1970s, during which time it has been known by a multitude of names including the Islamic Group, Al-Jihad al-Islami, the Jihad Group, and the Vanguards of Conquest. The initial goal of the organisation was to establish in Egypt an Islamic state, however the group's objectives expanded to include resisting, and actively targeting any Western influences in the Middle East. This latter endeavour led the EIJ to attack Israeli and American targets, both within Egypt and abroad. Following the incarceration of many EIJ members by Egyptian security forces in the 1980s the group split into two factions, one led by Abdul al-Zumar, the other led by the rising figure of Al-Zawahiri. Al-Zawahiri entered the public consciousness during his period of imprisonment, emerging as a passionate speaker condemning the treatment of prisoners and extolling the virtues of a "true" Islamic state.

While Zumar's faction dwindled into obscurity, the al-Zawahiri faction prospered. Significantly, since 1998 the EIJ has merged with Al-Qaeda and according to many researchers played a pivotal role in the selection of the World Trade Centre and the Pentagon as targets for the 2001 attacks. The link between the two organisations is not however a new phenomenon. EIJ moved their headquarters to Afghanistan following Al-Zawahiri's release from prison in 1984. From here the EIJ recruited many Afghan militants who would be trained in Mujahideen camps, before returning to undertake terrorist operations in Egypt. It is also worth noting that Al-Zawahiri's

EIJ militants, many of whom were young doctors and engineers, provided Al-Qaeda with a great deal of their expert knowledge and carved a name for themselves amongst the Afghan Arabs as the “thinkers and the brains”.

The transition into the Al-Qaeda led war against ‘Jews and Crusaders’ has not however been at all times a smooth one for al-Zawahiri’s EIJ. Some researchers have suggested that al-Zawahiri’s allegiance with Al-Qaeda caused another split within the EIJ between those supporting the move, and those who felt al-Zawahiri had become distracted from the original goal of overthrowing the Egyptian government.

In terms of perpetrated attacks, the EIJ is believed to be responsible for assassinating Egyptian President Anwar Sadat in 1981, as well as attempting to assassinate Interior Minister Hassan al-Alfi in 1993 and Prime Minister Atef Sedky in the same year.

Since his assimilation into Al-Qaeda in 1998 Al-Zawahiri went on to become in 2009 the organisation’s operational and strategic commander. After bin Laden’s death on 2 May 2011 Al-Zawahiri became Al-Qaeda’s official leader.

Gama'a al-Islamiya (IG) - Egypt

Gama'a al-Islamiyya, Egypt's largest militant group, has been active since the late 1970s, originally formed by the coming together of militant student cells following the renunciation of violence by the Muslim Brotherhood.

As is the case with many terrorist groups, Gama'a al-Islamiyya recruited many of its leaders from amongst the ranks of dissatisfied and radical students, and from the radical Islamist group Takfir wal-Hijra which was crushed by the Egyptian military in the 1960s, while the bulk of the membership originate from economically deprived regions, predominantly in the south of Egypt.

The emergence of radical Islamic terrorist groups in Egypt was widely linked to the renaissance of political Islam that has swept through much of the Arab world since late-1960s. Gama'a al-Islamiyya's individual brand of Islam is dictated by the spiritual leadership of Shaykh Umar Abd al-Rahman, a figure who diverged from the Muslim Brotherhood. Al-Rahman, despite spending many years behind bars, has also supplied a great deal of the group's strategic decision making.

Originally the self-proclaimed objective of Gama'a al-Islamiyya was to overthrow the Egyptian government, replacing it with an Islamic state. However its members have also been involved in religious crusades beyond Egypt, many taking part in the Afghan Jihad during the Soviet occupation of Afghanistan and the civil war that followed their withdrawal. Nonetheless the external wing, composed mainly of exiled members scattered across several countries, maintained its primary goal

to overthrow the Egyptian government of President Mubarak.

Since its formation the Gama'a al-Islamiyya has experienced fissures within its organisation, the first of which took place in 1997 following an attack on Western tourists at Luxor. The attack, planned to demonstrate the Egyptian government's powerlessness to protect foreigners, proved to be a political miscarriage and resulted in a backlash of public outrage towards the perpetrators rather than the government. Consequently a cease-fire was called by the group's then leadership, from which two factions emerged.

The first faction, led by Mustafa Hamza, supported the cease-fire, while the second, led by Refai Ahmed Taha, called for an immediate return to armed operations. Later Taha caused further fractures to emerge within Gama'a al-Islamiyya when he signed Osama bin Laden's declaration of war against ‘Jews and Crusaders’. The decision to join Al-Qaeda was not accepted by a large portion of Gama'a al-Islamiyya and has resulted in what might be described as the formation of radical and non-radical wings.

Following this split Taha's radical faction based in Afghanistan continued to have close associations with Al-Qaeda and the Egyptian Islamic Jihad (EIJ). Following the 9/11 attacks Taha's faction was targeted by US-led forces in Afghanistan and what remained of the faction is believed to have dispersed into Pakistan and various outlying regions, but may have regrouped.

In March 2002, members of the group's historic leadership remaining in Egypt declared the use of violence misguided and renounced acts of terrorism in the future. While this declaration was not accepted by leadership figures of the organisation's radical wing in foreign exile (some of whom have since announced their union with Al-Qaeda), such a move no doubt contributed to the Egyptian government's release of some 900 members in 2003, as well as up to 700 more in 2004.

At the height of its operational activity Gama'a al-Islamiyya conducted armed attacks against Egyptian security and other government officials, Coptic Christians, and Egyptian opponents of Islamic extremism.

The most notable attacks in Gama'a al-Islamiyya's history are those which targeted foreign tourists at Luxor in 1997, and the 1995 attempted assassination of the Egyptian President Hosni Mubarak in Ethiopia. Today the group is believed to have support in Cairo, Alexandria, and other urban centres within Egypt, as well as in foreign territories such as Afghanistan, Yemen, the UK and elsewhere in Europe.

In 2011 the group also established a political party known as the Building and Development Party, contesting the 2011–2012 elections as part of the Islamic Alliance and winning a total of 13 seats.

Turkey



Turkey is located at the crossroads of Europe and Asia and has been of strategic importance since even before the time of Alexander the Great who Hellenised the area which continued with the Roman rule and the transition into the Byzantine Empire, followed by the Turkification

of the region leading to the creation of the Ottoman Empire encompassing much of Southeastern Europe, Western Asia and North Africa. After the Ottoman Empire collapsed following its defeat in World War I, parts of it were occupied by the victorious Allies. The Turkish War of Independence, initiated by Mustafa Kemal Atatürk and his colleagues, resulted in the establishment of the modern Republic of Turkey in 1923, with Atatürk as its first President. Turkey is a democratic, secular, unitary, constitutional republic with a diverse cultural heritage. The country's official language is Turkish, a Turkic language, which is spoken by approximately 85% of the population. Turks constitute 70% to 75% of the population. The vast majority of the population is Muslim. The largest minority making up 18% are the Kurds, many of whom want to see a separate Kurdistan and support the PKK and other groups seeking secession and autonomy. Turkey's location between Asia and Europe, make it one of the most significant transit locations for drugs and human trafficking.

Turkey Designated Terrorist Organisations

In addition to the PKK, Turkey has designated¹⁴ the following active groups as terrorist organisations: Communist Workers Party of Turkey (TKP); Revolutionary People's Liberation Party-Front; Maoist Communist Party; Communist Party of Turkey/Marxist-Leninist; Marxist Leninist Communist Party; Revolutionary Communist Party of Turkey; Revolutionary Party of Kurdistan; Democratic Party of Kurdistan/North); Kurdish-Hezbollah also known as Kaplanclar; Great Eastern Islamic Raiders' Front and Hizb ut Tahrir. The Kurdistan Freedom Falcons (TAK) is not on the list despite being designated as a terrorist organisation by the US, EU and the UK because Turkey views the group as part of the PKK.

Kurdistan Workers Party (KADEK/KONGRA-GEL) - Turkey/Iraq

The Kurdistan Workers' Party (PKK) was founded in 1974 by Turkish left-leaning students of Kurdish descent.¹⁵ Ascribing to Maoist ideology the organisation sought to act as the vanguard of a revolutionary movement to secure an independent Kurdish state.

On its foundation the group asserted that a Kurdish state could only be created following the overthrow of the Turkish government, which it saw as an oppressive colonial power. The PKK held dual objectives, intending to both unite [the divided revolutionary left in Turkey] and secure an independent Kurdish state. In its early years the student led PKK established training camps in an area of Syrian-controlled Lebanon known as the Bekaa valley, and later in 1984 set up similar training camps in France, from where it launched a number of operations in European countries. Full-scale PKK insurgency within Turkey began in the early 1990s and the group successfully seized control of large swathes of countryside in the south-east. This campaign endured until 1999 when a cease-fire was called, an agreement that was to be officially retracted in 2004. In terms of organisational strength, the PKK was estimated in 1994 to have 10,000 to 15,000 members. The group's most notable income sources are believed to be derived from drug smuggling and extortion. Some revenue is also channelled through charities, while Iran, Iraq and Syria have also provided financial aid. High risk targets of PKK attacks have been Turkish government facilities and personnel, as well as any groups, including Kurds, thought to be collaborating with the regime. The scale of violence perpetrated by the PKK has led some to believe that more than 30,000 civilians perished as a direct result of their operations. Since 2002 the group has undergone numerous cosmetic name changes and has on several occasions proclaimed a commitment to non-violence while simultaneously continuing violent operations against the Turkish authorities. As a result fighting between Turkish and PKK forces has continued throughout the early 2000s, with Turkish forces frequently striking the Kurdistan region of Iraq, from which the PKK has launched many of its operations.

Today the PKK no longer campaigns for complete separation from the Turkish state, but rather champions a move towards a more democratic and confederalised Turkey. However in September 2012 fighting between PKK and Turkish forces reportedly escalated to new highs, demonstrating that the group remains a highly potent force with significant military capabilities. Recent peace negotiations between the PKK and the Turkish government were announced in 2013 with the PKK agreeing to a ceasefire and agreeing to move PKK fighters out of Turkey into mountain strongholds in Northern Iraq. It is thought the PKK may be willing to settle for greater autonomy, including constitutional and linguistic rights and to drop demands for an independent Kurdish state. A splinter group, the Kurdistan Freedom Falcons designated by the US in 2008 continues its violent struggle for Kurdish independence.

The PKK has used other names in order to suggest it has changed namely, the Kurdistan Freedom and Democracy Congress (KADEK) and the Kurdistan People's Congress (KONGRA-GEL)

Kurdistan Freedom Falcons

The Kurdistan Freedom Falcons (TAK), also known as the Kurdistan Freedom Hawks or the Kurdish Vengeance Brigade, is a militant group that has committed attacks throughout Turkey, operating in southern Turkey and northern Iraq with a goal of securing Kurdish secession from Turkey. It is unclear whether or not TAK is connected to any other Kurdish nationalist organisations, though it is believed they split off from the Kurdistan Workers Party (PKK) when they became dissatisfied with the group's tactics. Some Turkish security analysts have alleged that Bahoz Erdal may be the leader of the TAK. Most TAK attacks are directed against tourist areas in Istanbul, Ankara, and southern coastal resort areas. In the first three months of 2006, they claimed responsibility for eight bombings that killed two and injured 47 civilians. TAK has been designated as a terrorist organisation by the US, UK and by the EU.

Revolutionary People's Liberation Party (DHAKP)-Front - Turkey

The DHKP/C is a marxist, anti-western terrorist group that fought against previous Turkish regimes, considering them fascist and imperialist forces of the West, particularly the US and NATO and in particular the group has been intensely outspoken against US military operations in Afghanistan and Iraq. The group was designated as a US terrorist organisation in 2005.

Turkish Mafia - Turkey

Highly secretive and ruthless, the Turkish Mafia in some respects, mirror the Sicilian Mafia of years past, with its highly intricate code of honor based upon a patriarchal system of respect tracing its origins to the days prior to the Ottoman arrival. Encoded into an order, it became known as the Canun of Lek Dukagjeni. This code was religiously followed in the north of the country, where a clan system predominated life. Every aspect of social relations is embodied in the Canun. Based upon respect, family and loyalty, the code has been used by the criminal groups as a means to ensure allegiance. The extended family is given high priority and an attack upon one of its members constitutes a hukmarr_je, or blood feud, an attack upon the entire family or organisation. The ethnic requirement, though, is the highest priority. Similar to La Cosa Nostra, members entry obligates possible recruits to swear an oath of allegiance and secrecy, an omerta, or besa. The Turkish Mafia activities include drugs and refugee smuggling, arms trafficking, contract killing, kidnapping, false visa forgery, and burglary. Whilst Turkish criminal gangs had long existed they were a scattered and disorganised band of gangs, largely working for others. This changed though through a number of important developments which transformed them from local criminal gangs into international major operators to rival those in Russia, Italy and elsewhere. Firstly the campaign against the Italian Mafia by for example US Law Enforcement provided an opportunity for others, including the Turks to take up part of the drug trade previously controlled by the Ital-

ians. Secondly, the civil war in Yugoslavia which helped divert approximately 60% of Western Europe's heroin trade. From Central Asia and through the Middle East, the drug trade had long used Yugoslavia as a conduit for the rest of Europe for years. Realizing that they now required an alternate route, an organised Turkish Mafia quickly offered their services and together with the Albanian Mafia linked up to provide overland routes for drugs to travel from Turkey to Greece and then to Macedonia. From there on the coast in small craft, capable of avoiding detection travel either north towards the Dalmatian coast or across to Italy. The drugs that land in Italy do so with the assistance and blessing of the Sacra Corona Unita of Puglia, Italy taking a percentage of the profits. This type of trade and activity has increased and estimates suggest that the Turkish Mafia now control 70% of all illegal heroin trade bound for Austria, Germany and Switzerland. A great source of recruitment and local knowledge and support comes from the émigré communities located throughout Western Europe. Whether in UK, Italy, Austria, Germany, or Switzerland, either trafficked by the gangs already or ethnics legally resident from Turkey, have been sought out by organised crime groups for criminal activity. Many find it hard to assimilate and to find decent employment and are taken on as cheap labour in Turkish restaurants, cafes, and the like. For some the lure of working with the Mafia is hard to resist. While authorities are not certain as to who may control large sections of organised Turkish gangs, some information is known about the groups. One 'godfather' of the Turkish mafia is reputed to be a drug trafficker called Dau Kadriovski. Based in Turkey, Kadriovski reportedly has extensive links throughout Europe. Authorities also believe that Kadriovski may have links with the Ulkuculer or Grey Wolves. Despite efforts by law enforcement to curb his activities, Kadriovski continues to evade police. The most well known Turkish organised criminal gang however is the Ulkuculer or Grey Wolves.

Ulkuculer/Grey Wolves - Turkey

The Ulkuculer's formal name in Turkish is Ulkucu Hareket (The Idealist Movement). Members of the Ulkuculer are of Kurdish stock are designated as Cyngyraky Yylan, a variation of the Turkish word for rattlesnake. The Ulkuculer participate in a diverse range of criminal enterprises from human trafficking and prostitution to narcotics and gambling. They are close to and work with the Albanian Mafia, particularly the Bano Aldo Bare. Whilst secretive, the Ulkuculer is reportedly led by Abuzer Ugurlu who first emerged as a smuggler of arms, before moving on to more lucrative drug smuggling. The organisation was suspected by some of involvement in the murder of Pope John Paul II by the Turkish criminal Mehmet Ali Agca, the gang being already paid US\$1.7mio to kill the pope. Whilst the motives for the attempted assassination remain unclear, the leading claims had Russian and Bulgarian brokers as most likely involved, and not the Turkish Mafia though on-one has ultimately been held to account beyond Agca.

Asia



Asia, covering over 30% of the world's land area is also the most populous with 4.3 billion people (60% of the world's population). With diverse ethnic groups, cultures and environments, Asia is one of the most heterogeneous. Today its 46 countries contain very diverse economic and

political systems and historical ties many influenced by the European imperial era.

The name Asia dates back to classical antiquity with several theories but its provenance is ultimately unknown. Its perceived boundaries have changed over time and even today many different bodies have differing definitions. As well as having several geographical definitions for Asia as a whole its sub-regions can also cause confusion. For example all of Russia is deemed to be within Eastern Europe even though most of it is in Asia. The other sub-regions (as defined by the UN) include Central Asia, Western Asia, Southern, Asia Eastern Asia and South Eastern Asia. These classifications are very much historical/political constructs rather than obvious topographical boundaries such as the seas and oceans which bound Africa. To add to the confusion most European languages use the word 'Asian' to mean ethnic origin and which are often based on their own historical experiences. American English speakers take the word to mean someone from East Asia whilst British English speakers would regard an 'Asian' as someone from South Asia. For many centuries India and China were both at different times the largest economies in the world and European colonialism were mainly motivated by the desire to access these economies. The discovery of America came as a result of Western European countries wanting to get to India and the 'East' by a different route. Most of Asia up until the Second World War was in fact ruled by colonial powers and although China and Japan never were colonised they were in different ways profoundly affected by western imperialism.

Today Asia is the fastest growing economic area of the world with China as the second largest economy in the world. Indonesia is the 15th largest with South Korea 12th largest, Japan 4th largest and India 3rd largest. There are however wide disparities of wealth and income within and between some of the countries of Asia. What is clear is that in an era of globalisation the economic fortunes of the developed world are inextricably tied up with those of Asia and in particular China.

Southern Asia



South or Southern Asia is principally what is sometimes referred to as the Indian Sub-Continent i.e. Afghanistan, India, Pakistan, Bangladesh, Nepal, Bhutan Sri Lanka and the Maldives. The wider UN extended classification is used that includes Burma Iran and the China-Tibet Autonomous Region. The region has a population of approximately 1.8 billion which constitutes about 20% of the world's population. It is the most populous and most densely populated region in the world.

There is current and on-going violent conflict in Afghanistan, Pakistan, and the Indian Provinces of Jammu and Kashmir. In 2006 it was said that 232 of India's 640 districts suffered some degree of terrorism from insurgent and terrorist movements. In 2008 MK Narayanan the then Indian National Security Adviser said that but there were over 800 terrorist cells in India. The Government of India's Ministry of Home Affairs has listed 36 terrorist organisations. Pakistan also is regularly a victim of its own internal terrorist groups. Sri Lanka has emerged from a civil war and insurrection from Tamils and has been accused of acts of State Terrorism that include the massacre of civilians by several governmental and military organisations.

Sri Lanka has the highest GDP Per capita in South Asia with Afghanistan at the lowest. India is the economic giant of the region accounting for over 80% of the regional economy and is the world's 10th largest in nominal terms. Pakistan has the 5th largest GDP in the region

India is a member of the BRIC economies which are said to be at a similar stage of recent advanced economic development. However when taking income and wealth distribution into account many economists point out that South Asia is the poorest region in the world behind Sub Saharan Africa. According to the UN Multidimensional Poverty Index more than 25% of the world's poor, as defined by the index, live in Africa whilst 50% live in South Asia. The study showed that there were more poor people in eight Indian States than in the 26 poorest countries. World Bank poverty data in 2005 suggested that 40% of South Asia's population lived on less than the then International Poverty Line figure of US\$1.25 a day with the comparable figure in Sub-Saharan Africa of 50%.

Afghanistan

Ahmad Shah Durrani unified the Pashtun tribes and founded Afghanistan in 1747. The country served as a buffer between the British and Russian Empires until it won independence from nominal British control in 1919. A brief experiment in democracy ended in a 1973 coup and a 1978 communist counter-coup.

The Soviet Union invaded in 1979 to support a weak Afghan communist regime and withdrew 10 years later following strong opposition from an internationally supported anti-communist Mujahideen rebel force. A series of subsequent civil wars saw Kabul finally fall in 1996 to the Taliban, who had emerged in 1994 to end the country's civil war and anarchy. Following the 11 September 2001 terrorist attacks, US, Allied, and anti-Taliban Northern Alliance military action toppled the Taliban for sheltering Osama bin Laden and Al-Qaeda. Elections in December 2004 brought Hamid Karzai to the Presidency and he has since been re-elected in 2009. Despite gains toward building a stable central government, a resurgent Taliban and continuing provincial instability, particularly in the south and the east - remain serious challenges for the Afghan Government.

There is widespread corruption in Afghanistan and political instability impedes counterdrug efforts. Corruption remains a serious problem in Afghanistan with according to Transparency International, Afghanistan ranking equal 176 out of 176 countries in its 2012 Corruptions Perceptions Index, alongside North Korea and Somalia.

The presidential election for Afghanistan will take place in 2014, with current President Karzai not permitted to run for a third term. Corruption and ballot rigging last time in 2009 is also feared this time around. Candidates and frontrunners for the top positions include former main opposition leader Dr Abdullah Abdullah, who came second last time and a former foreign minister, Zalmay Rassoul, a close associate of Hamid Karzai and Ashraf Ghani, a former World Bank economist and former Finance Minister.

Crime in Afghanistan is present in various forms, and includes: corruption, contract killings or assassinations, kidnapping, drug trafficking, money laundering, and black marketeering. Since the downfall of the Taliban, crime rate has significantly increased in the capital city Kabul. Unemployment among a large portion of the population and rudimentary basic services are major factors behind crime and lawlessness. Armed robberies, burglaries, assault and kidnapping are regularly reported, particularly in the capital of Kabul. According to a 2013 Transparency International report, Afghanistan comes equal last in its Corruption Perception Index.

Despite government attention to eradicate poppy cultivation and after ten years of occupation by US led coalition forces not only is Afghanistan the largest

producer of opium in the world but according to the 2013 Afghanistan Opium Survey released in November 2013 Afghan Ministry of Counter Narcotics and the UNODC, opium poppy cultivation in Afghanistan rose 36% in 2013 to a record high.

Opium production amounted to 5,500 tons, up by almost a half since 2012. The area under cultivation rose to 209,000 hectares from the previous year's total of 154,000 ha, higher than the peak of 193,000 hectares reached in 2007. Almost 90% of opium poppy cultivation in 2013 remained confined to nine provinces in the southern and western regions, which include the most insurgency-ridden provinces in the country. Helmand, Afghanistan's principal poppy-producer since 2004 and responsible for nearly half of all cultivation, expanded the area under cultivation by 34%, followed by Kandahar, which saw a 16% rise.

Although lower than in 2012, opium prices continued to lure farmers at around US\$145 per kg, much higher than the prices fetched during the high yield years of 2006-2008. Worth around US\$950mio, or 4% of national GDP in 2013, the farm-gate value of opium production increased by almost a third. Together with profits made by drug traffickers, the total value of the opium economy within Afghanistan was significantly higher, implying that the illicit economy will continue to grow whereas a slowdown of the legal economy is predicted in 2014.

The UNODC called for an integrated, comprehensive response to the drug problem, with counter-narcotics efforts forming an integral part of the security, development and institution-building agenda. These record figures come ahead of the 2014 withdrawal of international forces from the country.

The Taliban and other antigovernment groups participate in and profit from the opiate trade, which is a key source of revenue for the Taliban inside Afghanistan. The growth in Afghanistan's banking sector has slowed considerably in recent years; and traditional payment systems, particularly hawala networks, remain significant in their reach and scale. The corrupt government and weaknesses in the banking sector incentivize the use of informal mechanisms and exacerbate the difficulty of developing a transparent formal financial sector in Afghanistan. The unlicensed and unregulated hawaladars in major drug areas such as Helmand likely account for a substantial portion of the illicit proceeds being moved in the financial system. Afghan business consortiums that control both hawaladars and banks allow criminal elements within these consortiums to manipulate domestic and international financial networks to send, receive, and launder illicitly-derived monies or funds intended for criminal, insurgent, or terrorist activities. Afghanistan is a source transit, and destination country for men, women, and children subjected to forced labour and sex trafficking, although domestic trafficking is more prevalent than transnational trafficking.

Special Focus 8 Al-Qaeda - Afghanistan/Pakistan



Al-Qaeda (AQ) is a broad-based militant Islamist organisation founded by Osama bin Laden in the late 1980s. The organisation began as a logistical network to support Muslims fighting against the Soviet Union during the Afghan War; members were recruited throughout the Islamic

world in a trans-national religious war-effort commonly known as the Afghan jihad. The philosophy underpinning the group is one of "defensive jihad", a concept under which Muslims are encouraged to take it upon themselves to fight perceived attacks on the Muslim faith across the world. As an extension of this view, the group aims to overthrow 'un-Islamic regimes' that they believe oppress their Muslim citizens and replace them with genuine Islamic governments. It is also their intention to expel US soldiers and Western influences from the holy territories of the Gulf and Iraq, as well as capture Jerusalem as a Muslim city. Further reported beliefs include the conviction that a Christian-Jewish alliance is conspiring to destroy Islam and that the killing of bystanders and civilians is religiously justified in jihad.

When the Soviets withdrew from Afghanistan in 1989, the organisation dispersed but continued to oppose what its leaders considered corrupt Islamic regimes and foreign (i.e., US) presence in Islamic lands. Based in Sudan for a period in the early 1990s, the group eventually re-established its headquarters in Afghanistan (c. 1996) under the patronage of the Taliban militia.

AQ merged with a number of other militant Islamist organisations, including Egypt's Islamic Jihad (EIJ) and the Islamic Group (IG), and on several occasions its leaders declared jihad (holy war) against the US. The organisation established camps for Muslim militants from throughout the world, training tens of thousands in paramilitary skills, and its agents engaged in numerous terrorist attacks, including the destruction of the US Embassies in East Africa and by AQAP a suicide bomb attack against the US Warship Cole in Aden, Yemen. AQ also aligns itself with and actively supports numerous terrorist groups throughout the world that are recognised as furthering their own goals. These include groups fighting Muslim governments with allegedly apostate rulers (Egypt under former President Mubarak, Algeria, post-2002 Afghanistan and Saudi Arabia),

groups fighting regimes perceived to oppress their Muslim citizens (Kosovo, India, Russia and Indonesia), and groups fighting to establish their own Islamic state (Palestine, Chechnya, Dagestan and Mindanao). AQ supports these groups in two ways; both by training group members in its camps and by sending its own members to help these groups in their local struggles. Training for its own members and for members of allied groups has focused on insurgent warfare in addition to the classic "terrorist" techniques that are usually associated with the group. Some experts even believe that the ratio of insurgent fighters to terrorists in Al-Qaeda camps may have been 15 to 1. American military officials have described the majority of those training in Al-Qaeda camps as "irregular ground combatants." Fighters such as these engaged US troops at Shai-e-Kowt and Tora Bora in Afghanistan.

In 2001, 19 militants associated with Al-Qaeda staged the September 11 attacks against the US. Within weeks the American government responded by attacking Taliban and Al-Qaeda forces in Afghanistan. Thousands of militants were killed or captured, among them several key members (including the militant who allegedly planned and organised the September 11 attacks), and the remainder and their leaders were driven into hiding.

The invasion of Afghanistan in 2001 challenged that country's viability as an Al-Qaeda sanctuary, compromising communication, operational, and financial linkages between the Al-Qaeda leadership and its vast network of militants. Rather than significantly weakening Al-Qaeda, however, these realities prompted a structural evolution and the growth of "franchising." Increasingly, attacks were orchestrated not only from above by the centralized leadership (after the US invasion of Afghanistan, based in the Afghan-Pakistani border regions) but also by the localized, relatively autonomous cells it encouraged. Such independent grassroots groups coalesced locally around a common agenda but subscribing to the Al-Qaeda name and broader ideology thus meant a diffuse form of militancy, and one far more difficult to confront. Sleeper cells embedded in several countries with indoctrinated members leading ordinary lives and activated at the behest of the terrorist commanders add further complexity to the problem of identification.

With this organisational shift, Al-Qaeda was linked whether directly or indirectly to more attacks in the six years following September 11 than it had been in the six years prior, including attacks in Jordan, Kenya, Saudi Arabia, Indonesia, Turkey, the UK, Israel, Algeria, and elsewhere. At the same time, Al-Qaeda increasingly utilised the Internet as an expansive platform for communication and recruitment and as a mouthpiece for video messages, broadcasts, and propaganda. Meanwhile, some observers expressed concern that US strategy centred primarily on attempts to overwhelm Al-Qaeda militarily was ineffectual, and at the end of the first decade of the 21st century, Al-Qaeda was thought to have reached its greatest strength since the attacks

of September 2001. On 2 May 2011, bin Laden was killed by US military forces after US intelligence located him residing in a secure compound in the cantonment town of Abbottabad, Pakistan, approx 110kms from the capital of Pakistan, Islamabad. The operation was carried out by a small team that reached the compound in Abbottabad by helicopter. After bin Laden's death was confirmed, it was announced by US President Barack Obama, who hailed the operation as a major success in the fight against Al-Qaeda. On 16 June 2011, Al-Qaeda released a statement announcing that Ayman al-Zawahiri, bin Laden's long-serving deputy, had been appointed to replace bin Laden as the organisation's leader.

In terms of financial structure AQ is not only a combatant organisation, it's also and most of all a confederation of militant organisations around the world and money is used to support and enhance this confederation. Money is therefore needed to fund, stabilise and leverage their support and to develop their reach. Over the years AQ has financially supported numerous entities, from Libya to the Philippines, from Indonesia to Somalia. Figures here range in millions of dollars. Money is also needed to pay for protection and asylum. Since 1991, AQ had to resettle in various countries after the opposition movement was banned from Saudi Arabia. It has been the same story in Sudan, Afghanistan, and now most likely in the tribal areas of Pakistan. Such expenditures will include Communication, Networks, Training facilities, Protection etc were estimated to utilise 90% of AQ operational funds. The remaining 10% being used to fund the planning and execution of terrorist attacks. Within a 10-year period, the financial support at the disposal of AQ or its sister organisations, received through direct donations or Zakat funds to charities or through various fraudulent schemes ranged from between US\$300mio and US\$500mio in total, a sum that is then commingled and often diverted or siphoned to groups that support terrorism. AQ's expenditures have decreased significantly since the 9/11 attacks, although it is impossible to determine to what extent. The organisation has also become decentralized and it is unlikely that a formal finance structure exists.

AQ no longer pays money to the Taliban (for safe haven or otherwise) and no longer operates extensive training camps in Afghanistan or elsewhere. It does still however provide operatives and their families with modest support and occasionally provides funds to other terrorist organisations, especially those in Southeast Asia. Intelligence analysts estimate that Al-Qaeda's operating budget may be only a few million dollars per year, although such estimates are only tentative.

Charities and the Islamic phenomenon of Zakat are the most important source of financial support for the AQ network, essentially because it is the most usual and unregulated way to raise donations, particularly in the Middle East though this has changed and been the subject of increased regulation and oversight. In several cases, money originating from Islamic banks and chari-

ties in the Gulf was moved through Western correspondents, whether banks or charities, before reaching their recipients. In that respect, much of the financial revenue of AQ was raised through legal means. Charitable giving, known as Zakat, is one of the five pillars of Islamic faith and represents a much broader notion of charity than that to which we in the West are accustomed. In many ways comparable to the Christian tithe, the Zakat also functions as a form of income tax, educational assistance, foreign aid, and expression of political support. The Western notion of the separation of civic and religious duty generally does not exist in Islamic cultures with religion also guiding temporal aspects of life. For instance the Saudi government has declared that the Koran and the Sunna tradition of Muhammad are to function as the country's constitution, and the clergy within Saudi Arabia wield enormous influence over the cultural and social life of the country. AQ's reliance on charities to raise, mask, transfer and distribute the funds it needs, has been put under close scrutiny by counter-intelligence and enforcement agencies around the world. These included more than 50 international and local charities, many of these charities were based or funded from the Gulf Region and/or from Afghanistan and/or Pakistan. These included the International Islamic Relief Organisation (IIRO) (Philippine and Indonesian branches), the Benevolence International Foundation, the Al Haramain Islamic Foundation (Bosnian and Serbian Offices), Blessed Relief (Muwafaq) Foundation, the Al-Akhtar Trust, the Afghan Support Committee, the Al-Rashid Trust, the Revival of Islamic Heritage, the Global Relief Foundation, Taibah Int, Al-Furqan, Sanabah Charitable Committee and the Rabita Trust (see Part 2, Section 7, Criminal Cases for more details).

Donors

Following the invasion of Afghanistan by Soviet forces and the establishment of the Arab Mujahideen in Afghanistan in 1980, wealthy AQ gulf businessmen, bankers and institutions forged the financial backbone of AQ by transferring or facilitating the transfer of funds to charities or fronts tied to the Mujahideen struggle. A number of these donors have been identified in post 9/11 US litigation as being sponsors of AQ, however all vehemently deny such accusations and it has to be said no findings against such persons by a US or other court have been made. Nevertheless it is believed that AQ can still draw on hardcore donors who knowingly fund it and sympathizers who divert charitable donations to it. The exact extent to which the donors know where their money is going remains unclear. Still, there are suspicions that some Gulf donors did know that the fundraisers really were connected to AQ. Donors, whilst still at the core of AQ's revenue stream, remain under extreme pressure. There is little debate that the killing and capture of numerous important AQ members has decreased the amount of money Al-Qaeda is able to raise and has made it more expensive and difficult to raise money. The May 2003 terrorist attacks in Riyadh, moreover, seem to have reduced AQ's available funds even more –some say drastically - for a number of rea-

sons; i) it appears that enhanced scrutiny of donors by government bodies, especially that of Saudi Arabia, has made the act of donation a great deal more arduous for would-be supporters. ii) Saudi law enforcement efforts have captured or killed AQ facilitators in the country and iii) the Saudi population following these attacks are less inclined to fund AQ generally.

Bin Laden's Fortune

According to the 9/11 Commission Report and contrary to popular myth, bin Laden did not support AQ through a personal fortune or a network of businesses. For many years, the reverse was thought true, that bin Laden did indeed have access to and bankrolled AQ through a vast personal inheritance or through the proceeds of the sale of his Sudanese businesses. bin Laden was alleged to have inherited approximately US\$300mio when his father died, funds used while in Sudan and Afghanistan. Following US and Saudi Intelligence Sharing and interviews with the bin Laden family members the myth of bin Laden's fortune was discredited. From about 1970 until 1993 or 1994, bin Laden received about US\$1mio p.a - adding up to a significant sum, to be sure, but not a US\$300mio fortune. In 1994 the Saudi government forced the bin Laden family to find a buyer for bin Laden's share of the family company and to place the proceeds into a frozen account. The Saudi freeze had the effect of divesting bin Laden of what would otherwise have been a US\$300mio fortune.

State Sponsorship

States sponsors may contribute to terrorist groups such as Hamas and Hezbollah but there is no credible evidence of state sponsorship of AQ.

Companies and Businesses

While there is little hard evidence, considerable anecdotal information exists suggesting that Al-Qaeda and its sympathizers ran businesses to support the terrorist network. Shortly after September 11, US investigators looked at several businesses in Yemen that were implicated in funding AQ. They named the Al Hamati Sweet Bakeries and two honey businesses, Al Nur Honey Press Shops and Al Shifa Honey Press for Industry and Commerce. The Treasury Department charged that these companies knowingly funnelled money to bin Laden as well as assisting in the transportation of arms for Al-Qaeda. Both these operations were still in business long after 9/11. It is suggested that when OBL relocated to Sudan in 1991, he used his close relations with the then extensive power of Islamic leader Hasan al-Turabi to set up several business ventures, and built relationships with Sudanese leaders of the National Islamic Front (NIF).

In concert with NIF members, bin Laden is alleged to have invested in several large companies and banks, and undertook civil infrastructure development projects. The network of businesses controlled by bin Laden allegedly included a bank, an import-export firm, several agricultural companies, and a construction company to build roads and airport facilities in Sudan. These businesses enabled him to offer asylum and employment to AQ

members, as well as providing bank accounts for several operatives. This revenue stream also allowed bin Laden to finance terrorist operations and facilities, investing predominantly in training camps and weapons.

During the early 1990s, Al-Qaeda ran a series of international businesses out of its safe haven in Sudan. Nevertheless, according to the 9/11 Commission Report bin Laden's assets in Sudan were not a source of revenue for AQ. bin Laden was reputed to own 35 companies in Sudan when he lived there from 1992 to 1996, but some may never have actually been owned by him and others were small or not economically viable. His investments were most likely designed to gain influence with the Sudanese government rather than serve as feasible income sources. When bin Laden was pressured to leave Sudan in 1996, the Sudanese government apparently expropriated his assets and seized his accounts, so that he left Sudan with practically nothing. Consequently when he moved to Afghanistan in 1996, his financial situation was dire; it took months for him to get back on his feet. While relying on the good graces of the Taliban, bin Laden reinvigorated his fund-raising efforts and drew on the ties to wealthy Saudi nationals that he had developed during his days fighting the Soviets in Afghanistan. Financial support was also gained from elsewhere in the world. In a report submitted to the UN Al-Qaeda and Taliban Sanctions Committee the Government of the Philippines indicated that Mohammed Jamal Khalifa, bin Laden's brother-in-law, had established within its borders, numerous businesses, corporations and charitable institutions there which had served as a network to fund the Abu Sayyaf Group as well as other extremist organisations. These reportedly included the Khalifa Trading Industries, ET Dizon Travel Pyramid Trading, Manpower Services and Daw al-Iman al-Shafee Inc. AQ operative, Wali Khan Amin Shah, established several shell companies in Malaysia, as did Hambali, who used a shell "import export" company called Konsojaya Trading Company as a front to conceal terrorism funding transactions.

Drug Trafficking

According to the 9/11 Commission Report, after reviewing the relevant intelligence on AQ's involvement in drug trafficking and interviewing the leading authorities on the subject, there has been no substantial evidence that AQ played a major role in the drug trade or relied on it as an important source of revenue either before or after 9/11. While the drug trade was an important source of income for the Taliban before 9/11, it did not serve the same purpose for AQ. Unlike AQ the Taliban were known to take a large cut from this US\$6bio drug trade. However, following the crackdown on charities, some experts believe that AQ may have come to rely more heavily on drug money.

Conflict Diamonds

Allegations that AQ has used the trade in conflict diamonds to fund itself remain similarly unsubstantiated. 9/11 Commission staff have evaluated the sources

of information for these various public reports alleging illicit trade in diamonds.. These include the reports of journalists, the UN, and certain non-governmental organisations investigating this issue. The FBI conducted an intensive international investigation into the conflict diamond claims, including interviews of key witnesses with direct knowledge of the relevant facts, and found no evidence of any substantial AQ involvement. The CIA came to the same judgment.

Kidnapping

In one of its training manuals, AQ refers to the "carrying out [of] threats (extortion) against other regimes if they do not give willingly". In this case "one or two assassinations should be carried out so that the regime would realize that we are serious about our threats". The same applies to international companies such as "pharmaceutical companies, airline companies, insurance companies and petroleum companies, big industrial companies and meat companies, fruit companies". Certainly in Iraq, since the beginning of the Iraq war, according to US government figures hundreds of foreigners from more than 10 different countries have been taken hostage. These numbers are small in comparison to the kidnappings of Iraqis, which at one time took place at the rate of 10-30 per day, mainly for purposes of ransom. Many of these kidnappings were carried out by common criminals and some by AQ. The average ransom paid by Iraqi families was thought to be approximately US\$30,000, with the amount rising to US\$100,000 for foreigners but increasing substantially higher for Western hostages. The Italian press reported that its government paid millions of dollars in ransom to free two aid workers and, later, journalist Giuliana Sgrena. Some criminals were believed to have sold their foreign captives to AQ or other extremist groups, which are believed to pay high bounties for Westerners, especially Americans. On 8 March 2006 the website of Al-Arabiya satellite news channel published an interview with Abu Hafs, described as an aide of Abu Musab al-Zarqawi, a Jordanian militant infamous for publicised beheadings of American citizens, explaining his group's treatment of hostages: "We are in a war zone, and we have four ways to deal with hostages: killing the hostages and beheading them when we can't find a religious reason to preserve their lives, which is decided by religious courts that we founded. Sometimes we resort to the second option, which is trading hostages for our own prisoners; there's a third option that we don't like but is followed out of necessity, which is demanding a ransom; the fourth is release of AQ prisoners if the court finds them innocent."

Fraud Schemes including Smuggling and Credit Card Fraud

It is believed that fraud schemes have been used by AQ cells particularly in Europe. An AQ cell in Spain allegedly used stolen credit card numbers and provided forged credit cards for the use of AQ cells in other countries. Similar activity was also reported in Belgium. That being said it should be noted that in the 9/11 case

the hijackers were less than knowledgeable in the use of the US financial system. For example, the teller who opened an account for Atta and al-Shehhi, two of the plot leaders, spent an hour with them, explaining the procedures for ATM transactions and wire transfers, and one branch refused to cash a cheque for al Shehhi on one occasion because he presented IDs with different addresses. This incident led the bank to issue a routine internal security alert to watch the account for possible fraud, but provided no basis for concern about serious criminality let alone terrorism .

Maritime Piracy

According to the International Maritime Bureau, both the frequency and the violence of piracy acts have increased in recent years. The traditional operating areas of maritime pirates are the Arabian Sea, the South Chinese Sea, the waters off the coast of West Africa and the Straits of Malacca. Links between these pirates and terrorists, whilst circumstantial, have been made by NATO.

Precious Commodities

Beyond the raising of finances, it is also crucial for AQ to safely and covertly deposit its assets. The crackdown on AQ financing may have led AQ, even before 9/11, to transfer a portion of its exposed assets into untraceable precious commodities. This process reportedly began as early as 1998 when freezing actions were first initiated in the US and EU against the Taliban. This reportedly included transfers into commodities such as gold, diamonds, tanzanite and other precious minerals. These precious commodities, while of high value, are also small in size and therefore easy to store and transport; qualities well suited to AQ purposes. Moreover, for the most part they retain their value consistently over long periods of time and can also be released into the market in small quantities to avoid arousing suspicion.

Financial Institutions

AQ itself probably did not use the formal financial system to store or transfer funds internally after it moved to Afghanistan appears to contradict the reference to conversion of funds into precious commodities in the preceding paragraph. Furthermore the Afghan banking system was rudimentary at best, and the increased scrutiny after the East Africa bombings and the UN resolutions against bin Laden and the Taliban made the use of such institutions problematic.

Bulk Cash Smuggling / Couriers

According to US Treasury, former Under Secretary Stuart Levey: "As the formal and informal financial sectors become increasingly inhospitable to financiers of terrorism, we have witnessed an increasing reliance by AQ and terrorist groups on cash couriers. The movement of money via cash couriers is now one of the principle methods that terrorists use to move funds." AQ use couriers because they provide a relatively secure way to move funds. Couriers are typically recruited from within AQ and can maintain a low profile, perhaps because

of their background, language skills, ethnicity, or documentation, and so, ideally, no outsiders are involved or have knowledge of the transactions. Indeed even the couriers usually do not know the exact purpose of the funds. A single courier or several couriers might be used, depending on the route and the amount of money involved. Money is collected from a hawaladar, financial facilitator, or donor, and taken to its destination. For example, AQ reportedly used a Pakistani-based money changer to move US\$1mio from the UAE to Pakistan, at which point the money was couriered across the border into Afghanistan.

The 9/11 transaction also provides a good example of Al-Qaeda's use of couriers. Khalid Sheikh Mohammad described as the "principal architect of 9/11 attacks" in the final Report of the National Commission on Terrorist Attacks Upon the US delivered a large amount of cash, perhaps US\$120,000, to the plot facilitator Abdul Aziz Ali in Dubai; Ali then used the cash to wire funds to the hijackers in the US. Since 9/11 core AQ operatives have relied on cash transactions involving trusted hawaladars and couriers. The hawala network that existed prior to 9/11 seems to have been largely destroyed. Several of the main hawaladars who were moving money for AQ before 9/11 have been detained, and the identities of others have been revealed in seized records. AQ may have developed relationships with other hawaladars, and it most likely uses them to move some of its money. However major cash transfers apparently are done by trusted couriers or, for added security, by the main operatives themselves. Some couriers may be carrying information (although not specific operational details) as well as cash. The use of couriers has slowed down AQs movement of money considerably, with the physical transportation of cash over long distances necessarily taking much longer than electronic transactions such as wire transfers. In addition, there is evidence that significant delays in moving money, especially to AQ operatives in far-flung parts of the world, have been caused by the limited supply of trusted couriers.

Today AQ is known to have cells operating worldwide, and has executed noteworthy attacks in Africa, Asia, Europe, and North and South America. AQ, in any form, remains a dangerous threat to peace and stability throughout the world.

Al-Qaeda largely operates through its 3 main affiliates; Al-Qaeda in the Arabian Peninsula (AQAP); Al-Qaeda Organisation in the Islamic Maghreb and Al-Qaeda Organisation in the Land of the Two Rivers but can also count as allies the following terrorist groups amongst others: Abu Hafs al-Masri Brigade; Abu Sayyaf Group; al-Gama'a al-Islamiyya; Ansar al-Islam; Armed Islamic Group; Eastern Turkestan Islamic Movement; Egyptian Islamic Jihad; Harakat ul-Mujahideen; Islamic Jihad Union (Uzbekistan); Islamic Movement of Uzbekistan; Jaish-e-Mohammad; Jemaah Islamiya; Lashkar-e-Taiba; Libyan Islamic Fighting Group; and the Taliban. It also operates by inspiring others who are not part of

any criminal organisation to become radicalised and to take independent action.

The Afzidi Network - Afghanistan/Pakistan

The Afzidi Network, based in the region transecting the northern Pakistan-Afghanistan border, is centred on clan affiliations inherent in the region's culture and social make-up. The region is home to a culturally and ethnically distinct group known as Pashtuns, to whom clan affiliations, a strict code of honour and martial traditions are a longstanding way of life. It is the centrality of clan loyalties to the region's culture that is credited in large part for the success of its affiliates in dominating the territory's drug trade, providing as it does an automatic level of cohesion absent in many other areas of the world. Nor is it wholly surprising that the region should boast an organisation capable of resisting the law enforcement of both indigenous and foreign governments; for centuries Pashtun tribes have successfully thwarted all incursions by foreign powers. For instance during British imperial reign in India, the North West Frontier Province was never fully conquered and became known amongst soldiers simply as "the Grim", so ferocious were its inhabitants.

In more recent times occupations by Russian forces and a US led coalition have both failed to quell insurgency in the region. Even today the Pakistani central government cannot operate in the North West Frontier Province without the permission of local clan leaders. Presently the Afzidi clan network specialises in the smuggling of heroin and other opium based narcotics. The profitable revenue garnered in this way has allowed the clan's leader, Haji Ayub Afzidi, to amass considerable personal wealth and construct a \$2 million luxury home in Pakistan's Landi Kotal area. For Afzidi the man, working life began rather inauspiciously as a truck driver. His first foray into criminal activity came with his successes smuggling gold.

During the 1980s Afzidi formed connections with the Pakistan military, using the channels of his smuggling network to aid in the supply of arms to Mujahideen rebels opposing Soviet rule in Afghanistan. These selfsame channels also allowed Afzidi to move opium out of Afghanistan and into Pakistan, where it was refined and manufactured into heroin. From Pakistan it would then be exported to other areas of the world.

While Afzidi has not proven immune to prosecution, his relationship with law enforcement is a complex one. In 1995 Afzidi was extradited to America, where in 1996 he was convicted of narcotics smuggling charges. Afzidi served 3 of the 5 year sentence, before being sent back to Pakistan, where he immediately faced another trial for exporting 6.5 tons of hashish seized by law enforcement personnel in Antwerp, Belgium. Afzidi received a sentence of 7 years imprisonment, however after just a few weeks he was released without explanation.

Special Focus 9

Taliban - Afghanistan



The Taliban, sometimes spelt Taleban, is an Islamist militant terrorist and political group that ruled large parts of Afghanistan and its capital, Kabul, as the Islamic Emirate of Afghanistan from 1996 until 2001. It gained diplomatic recognition from only three states:

Pakistan, Saudi Arabia, and the United Arab Emirates. The predominantly Pashtun Taliban emerged in the latter part of 1994 as a 'messianic' movement made up of talib (students) from Madrassas, who were living as refugees in Pakistan. The group first came to prominence in 1994, when they were appointed by the Pakistani administration to protect a convoy attempting to open up a trade route between Pakistan and Central Asia.

The origin of the Taliban movement in Southern Afghanistan can be traced back to another incident in the same year, when a group of talib from the Darul Uloom Haqqania madrassa in Akora Khattak in Pakistan's North Western Frontier Province (NWFP), led by their teacher, Mullah Mohammed Omar, successfully battled a local Mujahideen 'commander' who had reportedly assaulted three women in Kandahar. Gradually, the Taliban, amply supported by Pakistan, evolved into a military force and went on to capture a large part of Afghanistan, after overthrowing the regime of Burhanuddin Rabbani. Their military campaign had rapid successes and in the first three months, they captured 12 out of the 36 regions of Afghanistan. These campaigns involved little hard fighting, as commanders simply switched sides after lucrative arrangements with the Taliban had been hammered out. These successes were primarily in the Pashto belt where the group could rely on considerable support from its ethnic community. Having established control over a majority of the poppy fields located in Southern Afghanistan, they began to expand westward towards Herat and northward towards Kabul. In the captured areas, the Taliban imposed strict "Islamic" laws and also disarmed the populace. In 1996, they stormed and captured Kabul, the capital of Afghanistan and immediately imposed their version of Sharia law (Islamic law). Perhaps most striking amongst the violence perpetrated by the Taliban was the torturing and public hanging of former President Najibullah, who had taken shelter in the UN premises. By September 1996, the Rabbani regime had also left Kabul without any resistance and the Taliban militia had assumed power in Afghanistan. The Taliban by that time were controlling 27 provinces of Afghanistan, and

the remaining three in the north were under the control of Uzbek-warlord Abdur Rashid Dostum. As a result of their many military successes, the Taliban's ranks had swelled over from a mere 2,500 to over 30,000 cadres.

The Taliban is widely acknowledged to be a creation of Pakistan and its external intelligence agency, the Inter Services Intelligence (ISI). This factor goes a long way in explaining the swift military successes of the Taliban against the non-Pashtun Afghan forces in campaigns in which both Pakistani Army officers and men (serving as well as retired) were involved. The Taliban's military campaign in Afghanistan commenced after an announcement by Pakistan that it would open a trade route through Afghanistan to Central Asia (former Soviet Central Asian Republics: Tajikistan, Uzbekistan, Turkmenistan). Pakistan ascertained that the Tajik-dominated government in Kabul posed a threat to their ambitions for a trade route through the area by keeping the Pashtuns, uncontrolled by any state, in a condition of agitation. However, the stakes for both Pakistan and Saudi Arabia were much more than trade routes; potentially lucrative oil and gas pipelines were also involved.

While in power, the Taliban enforced one of the strictest interpretations of Sharia law ever seen in the Muslim world. It was however a doctrine that received both support and criticism from the Islamic community; Al-Qaeda for instance reinforced the regime with militants from across the Middle-East and Central Asia, while some Muslim scholars condemned the Taliban for their opposition to the education of women. Indeed the Taliban's ill-treatment of women became notorious amongst the international community. Nonetheless the Taliban maintained allies in the Arab community, Pakistani's military and a community of Islamic militants across Arab and Central Asian countries. The high level of support for the Taliban regime from the more fundamental elements of the Islamic community is well illustrated by the fact that in 2001 as they continued to battle Afghanistan's remaining anti-Taliban forces, amongst a 45,000 strong Taliban force, only an estimated 14,000 were Afghans; the rest were drawn from other nationalities, prominently from Arab countries and Pakistan.

After the September 11 attacks, the US made the following demands of the Taliban, and refused to discuss them: Deliver to the US all of the leaders of Al-Qaeda. Release all foreign nationals who have been "unjustly imprisoned". Protect foreign journalists, diplomats, and aid workers. Close immediately every terrorist training camp, hand over every terrorist and their supporters to appropriate authorities, and allow the US full access to terrorist training camps for inspection. The US petitioned the international community to back a military campaign to overthrow the Taliban. The U.N. issued two resolutions on terrorism after the Sept. 11 attacks. The resolutions called on all states to "[increase] cooperation and full implementation of the relevant international conventions relating to terrorism" and specified consensus recommendations for all countries. The

Security Council did not however authorize military intervention in Afghanistan of any kind, and nowhere in the UN resolutions did it say military operations in Afghanistan were justified or conformed to international law. Despite this, NATO approved a campaign against Afghanistan as self-defence against armed attack. On September 21, the Taliban responded to the ultimatum, promising that if the US could bring evidence that bin Laden was guilty, they would hand him over, stating that they had no evidence linking him to the September 11 attacks. On September 22, the United Arab Emirates, and later Saudi Arabia, withdrew recognition of the Taliban as Afghanistan's legal government, leaving neighbouring Pakistan as the only remaining country with diplomatic ties. On October 4, the Taliban agreed to turn bin Laden over to Pakistan for trial in an international tribunal that operated according to Islamic Sharia law, but Pakistan blocked the offer as it was not possible to guarantee his safety. On October 7, the Taliban ambassador to Pakistan offered to detain bin Laden and try him under Islamic law if the US made a formal request and presented the Taliban with evidence. A Bush administration official, speaking on condition of anonymity, rejected the Taliban offer, and stated that the US would not negotiate their demands.

As a response to the attacks of September 11 2001 the Taliban regime was overthrown by the US led military campaign known as Operation Enduring Freedom. The US was supported by the International Security Assistance Force (ISAF), a fighting force made up of soldiers from the member states of the North Atlantic Treaty Organisation. The Taliban mostly fled to neighbouring Pakistan where it regrouped as an insurgency movement to fight the Islamic Republic of Afghanistan (established in late 2001) and the NATO-led International Security Assistance Force (ISAF).

Today the Taliban operate in Afghanistan and northwest Pakistan. US officials say one of their headquarters is in or near Quetta, Pakistan. The Taliban engage in attacks against the civilian population; according to a report by the UN, the Taliban were responsible for 2,477 civilian casualties (76% of all casualties) in the first six months of 2010.

Noorzai Organisation - Afghanistan/Pakistan

Since around 1990 Hajji Bashir Noorzai, an Afghan drug lord who controlled opium fields in Afghanistan, led an international-heroin trafficking organisation, producing the class A drug in Afghanistan and Pakistan, from where it was smuggled to other countries, including the US. Opium was first transported from fields in Afghanistan to Noorzai's laboratories in Pakistan, where it was made into heroine. This involvement in the illicit drugs trade, estimated by the Centre for Strategic and International Studies in Washington to be worth \$28 million annually, allowed him to mobilize forces against the Russian occupation of Afghanistan in the 1980s, and following their withdrawal to govern western Kandahar with a de facto administration. Politically

Noorzai was aligned with the Taliban in Afghanistan during their rule, providing through his organisation weapons, manpower and demolition services to the party. The strength of the allegiance between the Taliban and Noorzai is clearly demonstrated by the Afghan governments seizure of a truck-load of morphine in 1997; a cargo that was speedily returned to Noorzai with the personal apologies of Mullah Mohammad Omar, leader of the Taliban. It is also believed by the Centre for Strategic and International Studies that Noorzai acted as the primary heroin supplier for bin Laden. The allegiance between Noorzai and the Taliban was not however seemingly permanent, with Noorzai meeting US military personnel in 2001. In 2002 Noorzai demonstrated his break with the Taliban when he handed over 15 truckloads of their weaponry to the US. These weapons were alleged to have been hidden in his tribe's territory by the Taliban in order to resist the US led invasion. In 2005, despite his previous cooperation with the US, Noorzai was arrested by agents of the Drug Enforcement Administration in New York¹⁶ and stood trial for his role in establishing and directing a narcotics distribution network that encompassed the US capital from as early as 1990. The Grand Jury indictment of 2005 against Noorzai in the US stated that the Noorzai Organisation met in Pakistan in 2001 to discuss methods of transporting heroin to the US. In trials that reached their conclusion in 2009 Noorzai was found guilty of conspiracy to import US\$50mio worth of heroin into the US and other countries, manufacturing heroin, and one count of distributing heroin. On 3 April 2009 the man dubbed the "Pablo Escobar of heroin trafficking in Asia" was sentenced to life imprisonment by a US Judge.

The Khan Cartel - Afghanistan/Pakistan

This drug manufacturing and smuggling organisation is led by Haji Juma Khan, an ethnic Baluch from the Nimroz Province of Afghanistan. Like Noorzai, Khan is known to have strong links with the Taliban. During the period of Taliban rule in Afghanistan Khan operated as a provincial drug smuggler, however in the power vacuum that followed the ruling party's fall he rose to national prominence. For a short period Khan was detained by US forces after their conquest of the country, however he was soon released despite an appreciation of his involvement in drug trafficking. It is believed by many sources that Khan then went on to run the opium distribution network of the Taliban insurgents, thereby financing continued resistance to coalition forces in the region. The headquarters of Khan's operations were located under the cover of his travel agency in Quetta, Pakistan. Arrested in 2008 in Indonesia, he was deported to America to face trial under federal narco-terrorism laws. The waters of the trial have however been muddied somewhat by the revelation that Khan has served as an American informer over many years and plea negotiations between Khan and US authorities continue still. In the meantime, Imam Bheel is thought to have taken over the operation, himself at large though designated as a drug kingpin by US authorities in 2009.

Pakistan



The Islamic Republic of Pakistan sits at the crossroads of the strategically important region of South Asia, Central Asia and Western Asia bordering the Arabian Sea, between India on the east and Iran and Afghanistan on the west and China in the north.

Pakistan covers an area which is slightly less than twice the size of the US State of California. With a population of over 190 million people, it is the sixth most populous country in the world and has the largest Muslim population after Indonesia. The national language of Pakistan is Urdu but Urdu and English both are commonly used for official purposes. The country remains predominantly rural with almost two thirds of the population living in rural areas. The province of Punjab is the largest province on population basis.

Historically the territory of modern Pakistan has been ruled by numerous empires and dynasties and underwent successive invasions in subsequent centuries from the Persians, Greeks, Scythians, Arabs, Afghans, and Turks. The British came to dominate the region in the 18th century. In 1947 the partition of British India amongst the largest and most tragic displacement of people in the world history, created the independent Muslim state of Pakistan. However, the separation of the Muslim dominated Pakistan and Hindu India did not lead to a satisfactory resolution of the territorial issues and both countries fought three wars with the last of which in 1971 resulted in East Pakistan becoming a separate state of Bangladesh. India's nuclear weapons testing were seen as a threat to Pakistan which in turn conducted its own nuclear tests. Today both States are Nuclear States.

Economically, in contrast to its arch rival India, decades of internal political disputes and low levels of foreign investments have resulted in slow growth and underdevelopment in much of Pakistan. Agriculture accounts for more than one-fifth of output and two-fifths of employment. The UN estimated poverty in 2011 at almost 50% of the total population. Remittances from overseas workers, averaging about US\$1 bio a month (as of 2011) remain a crucial source of income for Pakistan's economy.

Pakistan faces significant risks of money laundering and even more significant risks of terrorism financing. Authorities acknowledge that Pakistan's economy is abused to support terrorist financing and that a significant source of terrorist funds is derived from the proceeds of crime (including bank robbery, kidnap for ransom, and

proceeds of drug trafficking flowing from Afghanistan). Pakistan is a significant transit area for Afghan drugs, including heroin, opium, and hashish, bound for Iran, Western markets, the Gulf States, Africa, and Asia. Authorities identified also cases of cash couriers and the misuse of charities/non-profit organisations as facilitating terrorist financing. While charities/non-profit organisations play a very important role in Pakistan's economy and society, parts of the non-profit organisation pose a significant terrorist financing risk, in particular in border regions with high level of terrorist activity.

Pakistani authorities are widely thought to have had ties to domestic militant groups that have largely focused their efforts abroad, as in Afghanistan and India, but post 9/11 the pressure to shut down support and to counter the Taliban and Al-Qaeda has placed the Pakistan authorities in a difficult position. Whilst the official position of the Pakistan government is to support the so called war on terror, it was in May 2011, Al-Qaeda leader bin Laden was killed by a US raid at a compound not far from Islamabad, raising new questions about Pakistan's commitment to fighting terrorism. Meanwhile, leadership elements of Al-Qaeda and the Taliban, along with other terrorist groups, have made Pakistan's semi-autonomous tribal areas their home, and now work closely with a wide variety of Pakistani militant groups, like the Haqqani Network, which in September 2012 was added to the US list of designated terrorist organisations.

Whilst there are many terrorist groups operating out of Pakistan, most tend to fall into one of five distinct categories as laid out by Ashley J. Tellis, a senior associate at Carnegie Endowment for International Peace, in a January 2008 testimony before a US House Foreign Affairs subcommittee. These are, sectarian groups engaged in violence within Pakistan; Anti-Indian groups operating with the alleged support of the Pakistani military and the intelligence agency Inter-Services Intelligence (ISI) and are largely active in Kashmir; Afghan Taliban; Al-Qaeda and its affiliates and the Pakistan Taliban.

Even with 5 broad categories there are some other militant groups that do not fit into any of the above categories—for instance, secessionist groups such as the Balochistan Liberation Army in the southwest province of Balochistan. Also, a new militant network, often labeled the Punjabi Taliban, has gained prominence after the major 2008 and 2009 attacks in the Punjabi cities of Lahore, Islamabad, and Rawalpindi and groups based in North Pakistan trying to agitate in the Central Asian Republic.

Hizb-e Islami Gulbuddin - Pakistan/Afghanistan

Hizb-e Islami Gulbuddin (HIG) emerged in 1977, founded by Gulbuddin Hekmatyar to liberate Afghanistan from the influence of foreign forces, overthrow the Afghan government, and establish a fundamentalist Islamic state. Based in Eastern Afghanistan and the tribal areas in Western Pakistan, HIG was known to be one

of the most radical mujahideen groups in the Afghan resistance during the Soviet occupation, with close ties to the Taliban, bin Laden and Al-Qaeda. Though anti-American in principle, Hekmatyar displayed pragmatism in accepting millions of dollars worth of American funding and equipment to help the Mujahideen fight the Soviets in Afghanistan. In the early 1990s, HIG operated several terrorist training camps in Afghanistan. After training, terrorists would be sent to assist Mujahideen in other parts of the world where there was religious conflict. Following bin Laden's expulsion from Sudan in 1996, Hekmatyar offered bin Laden safe haven. Since the US-led coalition invaded Afghanistan in 2001, Hizb-e Islami Gulbuddin has led terrorist attacks against the US, its coalition partners, the Afghan Transitional Administration (ATA) and the UN and NGOs as well.

Jamiat-e-Islami - Pakistan/Afghanistan

Jamiat-e Islami was an Afghan political party, whose military wing was established and led in 1979 by Ahmad Shah Massoud, the key Afghan resistance leader against Soviet occupation, to fight the Communist government and their Soviet allies. This group grew to control multiple provinces and included thousands of fighters. The Soviet Army launched a series of major offensives to attempt to destroy their forces, but they were unable to engage most of Massoud's men. After the withdrawal of the Soviet troops in 1988, the Mujahideen groups continued to wear down government forces; in 1992 the communist government collapsed entirely. Jamiat's forces were among the first to enter Kabul. Meanwhile, a peace and power-sharing agreement among the leadership of the Afghan political party leaders led to a tentative agreement to appoint Burhanuddin Rabbani, who had spent the civil war in exile, as interim president. The peace agreement was called the Peshawar Accords.

Gulbuddin Hekmatyar however, did not support the peace agreement despite the fact that he was repeatedly offered the position of prime minister. Subsequently his Hezb-e Islami Gulbuddin attacked the new interim government and the capital of Kabul. With other groups entering the conflict such as Hezb-i Wahdat and Ittihad-i Islami as well as Junbish-i Milli fighting against the Afghanistan Government, mainly for control of Kabul, the conflict would allow the Taliban, to consolidate its control of much of southern Afghanistan and then to advance on Kabul.

In March 1995, Massoud handed the Taliban their first major loss but they regrouped and together with bin Laden's forces, they launched another offensive in mid-1996, which led Massoud to retreat and hand Kabul to the Taliban. Following the capture of Kabul, the major Mujahideen factions put aside their feuds and formed the United Islamic Front for the Salvation of Afghanistan (the United Front), commonly known in the west as the Northern Alliance, with Rabbani, officially becoming its political leader. On 9 September 2001, just

two days before Al-Qaeda's attack on America, Massoud was assassinated by two suicide bombers. Immediately afterwards Taliban forces launched a major offensive against Northern Alliance positions. Mohammed Qasim Fahim was chosen to succeed Massoud as leader of Jamiat's military wing and repulsed the Taliban offensive. With extensive assistance from an American-led coalition in October and November 2001 Northern Alliance forces recaptured most of Afghanistan. Jamiat-e-Islami, amongst others given its anti-Soviet stance is designated by the Russian Federation as a terrorist organisation.

Quetta Shura - Pakistan/Afghanistan

Quetta Shura is a militant organisation composed of the top leadership of the Afghan Taliban, based since about 2001 in Quetta in Balochistan province of Pakistan. It was formed after forces led by the US attacked the Taliban in Afghanistan in November 2001, when the senior leadership of Taliban including Mullah Mohammed Omar, the spiritual leader of Taliban and one time Amir-al-Mu'min of Afghanistan escaped. Baluchistan is a province in Western Pakistan, is off-limits to the Pakistani military because ethnic Baluchs have fiercely resisted central government intrusion. American officials believe that the Quetta Shura gets support from parts of Pakistan's Inter-Services Intelligence (ISI) and its senior leaders are in hiding in Pakistan as some of its senior officials believe that leaders such as Mullah Omar would be valuable assets if the Taliban were to regain power after a withdrawal of US forces from Afghanistan.

Tehrik-e Taliban Pakistan/Pakistan Taliban (TTP) - Pakistan/Afghanistan

Tehrik-e Taliban Pakistan (TTP) is a Pakistan-based terrorist organisation formed in 2007 in opposition to Pakistani military efforts in the Federally Administered Tribal Areas. Previously disparate militant tribes agreed to cooperate and eventually coalesced into the TTP. TTP was led by Hakimullah Mehsud since August 2009, until his death in a US drone attack in November 2013. TTP's goals include overthrowing the Government of Pakistan by waging a terrorist campaign against the civilian leader of Pakistan, its military, and NATO forces in Afghanistan. TTP uses the tribal belt along the Afghan-Pakistani border to train and deploy its operatives, and the group has a symbiotic relationship with Al-Qaeda. TTP draws ideological guidance from AQ, while AQ relies on TTP for safe haven in the Pashtun areas along the Afghan-Pakistani border. This arrangement gives TTP access to both AQ's global terrorist network and the operational experience of its members.

TTP has carried out and claimed responsibility for numerous terrorist acts against Pakistani and US interests, including a December 2009 suicide attack on a US military base in Khowst, Afghanistan, which killed seven US citizens, and an April 2010 suicide bombing against the US Consulate in Peshawar, Pakistan, which killed six Pakistani citizens. TTP is suspected of being involved in the 2007 assassination of former Pakistani Prime Minis-

ter Benazir Bhutto. TTP claimed to have supported the failed attempt by Faisal Shahzad to detonate an explosive device in New York City's Times Square on May 1, 2010. TTP's claim was validated by investigations that revealed that TTP directed and facilitated the plot. Throughout 2011, TTP carried out attacks against the Government of Pakistan and civilian targets, as well as against US targets in Pakistan. Attacks in 2011 included: a March bombing at a gas station in Faisalabad that killed 31 people; an April double suicide bombing at a Sufi shrine in Dera Ghazi Khan that left more than 50 dead; a May bombing of an American consulate convoy in Peshawar that killed one person and injured twelve; a May siege of a naval base in Karachi; the May assassination of the PNS Mehran Saudi diplomat in Karachi. On 12 May 2011, the Pakistani Taliban claimed responsibility for bombing a paramilitary academy that killed eighty people and injured more than 100 and a September attack against a school bus that killed four children and the bus driver.¹⁷ TTP is believed to raise most of its funds through kidnapping for ransom and operations that target Afghanistan-bound military transport trucks for robbery. Such operations enable TTP to steal military equipment, which they then sell in Afghan and Pakistani markets.

Haqqani Network - Pakistan/Afghanistan

The Haqqani Network, whose operations and relations straddle the Afghanistan, Pakistan border has proven a valuable ally for some of the Pakistan Taliban's (TTP) illicit pursuits. The Haqqanis have not only fought alongside the TTP and Afghan Taliban in Afghanistan, they have also served as an influential mediator between the TTP and officials in Islamabad. Pakistan has long been a beneficiary of the Haqqanis who have helped Islamabad manage militant groups in the region and provided leverage against India in the struggle over Kashmir. Maulvi Haqqani and his son Sirajuddin Haqqani led the group first established to fight the Soviet Invasion of Afghanistan. Two notable foreign fighters both began their careers as volunteers for the Haqqanis, being trained to fight the Soviets. These were bin Laden and his mentor Abdullah Azzam. Later Al-Qaeda and the Haqqani Network evolved together and have remained intertwined with the main ideological difference being Al-Qaeda's global aspirations versus the Haqqani's preferring local ones. In September 2012 the US designated the network a US foreign terrorist organisation. After this announcement the Pakistani Taliban issued a statement informing that the Haqqani Network was not a separate organisation but a member of the TTP. The Network's funding is from local extortion and from private donations.

Tahreek-e-Nafaz-e-Shariat-e-Mohammadi - Pakistan/Afghanistan

The Tehreek-e-Nafaz-e-Shariat-e-Mohammadi (TNSM); (Movement for the Enforcement of Islamic Laws) was founded in 1992 with the primary objective of the imposition of strict Sharia Law in Pakistan, on the lines of the Taliban in Afghanistan.

The TNSM was one of five terrorist groups that were proscribed by former President Pervez Musharraf in January 2002. Maulana Sufi Mohammed (now imprisoned in Pakistan) is the leader of the TNSM. He was an active leader of the Jamiat-e-Islami in the 1980s. He quit the Jamiat in 1992 to form the TNSM. He is reported to have organised thousands of people to fight the Northern Alliance (NA) in Afghanistan after the defeat of the Taliban in 2001. However, a majority of them were either killed or arrested by the NA in Afghanistan. Some, including Sufi Mohammed, managed to return to Pakistan, only to be arrested. Since Sufi Mohammad's imprisonment, his son-in-law Maulana Fazalullah is reportedly now leading the TNSM.

The TNSM headquarters is located in the North West Frontier Province (NWFP), operates primarily in the tribal belt, such as Swat and the adjoining districts of the NWFP. Since the imprisonment of Sufi Mohammed and the proscription by the Pakistani Government, the TNSM has been largely defunct. The Government believes that the TNSM has links with the Taliban militia in Afghanistan.

Lashkar I Jhangvi (LJ) - Pakistan/Afghanistan

Lashkar I Jhangvi was designated as a US Foreign Terrorist Organisation on 30 January 2003, Lashkar I Jhangvi (LJ) is the militant offshoot of the Sunni Deobandi sectarian group Sipah-e-Sahaba Pakistan. LJ focuses primarily on anti-Shia attacks and other attacks in largely Sunni Pakistan and Afghanistan, and was banned by Pakistan in August 2001 as part of an effort to rein in sectarian violence. Many of its members then sought refuge in Afghanistan with the Taliban, with whom they had existing ties. After the collapse of the Taliban as the ruling government in Afghanistan, LJ members became active in aiding other terrorists, providing safe houses, false identities, and protection in Pakistani cities, including Karachi, Peshawar, and Rawalpindi. LJ works closely with the Pakistani Taliban (TTP).

LJ specialises in armed attacks and bombings and has admitted responsibility for numerous killings of Shia religious and community leaders in Pakistan.

In January 1999, the group attempted to assassinate former Prime Minister Nawaz Sharif and his brother Shabaz Sharif, Chief Minister of Punjab Province. Media reports have also linked LJ to attacks on Christian targets in Pakistan, including a March 2002 grenade assault on the Protestant International Church in Islamabad that killed two US citizens. Pakistani authorities believe LJ was responsible for the July 2003 bombing of a Shia mosque in Quetta, Pakistan. Authorities also implicated LJ in several sectarian incidents in 2004, including the May and June bombings of two Shia mosques in Karachi, which killed more than 40 people. LJ was very active in 2011. The most notable attack occurred on December 6, in Kabul, Afghanistan, when a suicide bomber detonated an improvised explosive device in a

crowd of Shia mourners, killing 48 civilians – including 12 children – and wounding 193. LJ claimed responsibility. In a particularly tragic attack on 29 September, in Balochistan, LJ operatives ordered Shia pilgrims off a bus and shot dead 29 victims. An hour after the initial attack, gunmen killed family members travelling to retrieve the victims of the first attack. Additional 2011 attacks included: a January firebombing attack that injured four police officers, and six civilians, including three children; a May attack that killed eight civilians and wounded 15; another May attack that killed two police officers and wounded three; and a July 30 attack that killed 11 civilians and wounded three.

Funding comes from wealthy donors in Pakistan as well as the Middle East, particularly Saudi Arabia. The group also engages in criminal activity to fund its activities, including extortion and protection money.

Islamic Jihad Union (IJU) - Pakistan/Afghanistan

The Islamic Jihad Union was designated as a US Foreign Terrorist Organisation on 17 June 2005, The Islamic Jihad Union (IJU) is a Sunni extremist organisation that splintered from the Islamic Movement of Uzbekistan (IMU). The IJU, based in Pakistan, primarily operates against Coalition Forces in Afghanistan and continues to pose a threat of attacks in Central Asia. The group claimed responsibility for attacks in March and April 2004, targeting police at several roadway checkpoints and at a popular bazaar, killing approximately 47 people, including 33 IJU members, some of whom were suicide bombers. In July 2004, the group carried out near-simultaneous suicide bombings of the Uzbek Prosecutor General's office and the US and Israeli Embassies in Tashkent. In September 2007, German authorities disrupted an IJU plot by detaining three IJU operatives, including two German citizens. Foreign fighters from Germany, Turkey, and elsewhere in Europe continued to travel to the Afghan-Pakistan border area to join the IJU to fight against US and Coalition Forces.

Sipah-e-Sahaba/Millat-e-Islamia - Pakistan

Earlier termed Anjuman Sipah-e-Sahaba, the Sipah-e-Sahaba Pakistan (SSP) is a Sunni terrorist group that has primarily targeted the minority Shia community in Pakistan. The group in its earlier times contested elections in 1993 before being proscribed by then President Pervez Musharraf in 2002. The group is reported to have been renamed as Millat-e-Islamia Pakistan after the proscription. The SSP is reported to have approximately 3,000 - 6,000 trained activists who indulge in various kinds of violent sectarian activities, which are primarily directed against the Shias. Most SSP activists come from the Punjab.

The SSP is also reported to be closely linked to the Jaish-e-Mohammed (JeM), a Pakistan-based terrorist outfit active in Jammu and Kashmir. The SSP draws support, inspiration and assistance from various political parties in Pakistan, primarily the Jamiat-e-Islami (JeI) and the Jamaat-Ulema-e-Islam (JuI). The JuI is associ-

ated with running a large number of Madrassas all over Pakistan from where recruits for the HuM, SSP and Taliban are provided. The SSP reportedly receives significant funding from Saudi Arabia and through wealthy private sources in Pakistan. Funds are also acquired from various sources, including Zakat and donations from various Sunni extremist groups. Other sources include donations through local Sunni organisations and trusts, Madrassas and study circles, and contributions by political groups. Most of the foreign funded Sunni Madrassas in Pakistan are reportedly controlled by the SSP.

Kashmir

The independence of India in 1947 resulted in partition in the Indian sub continent, largely divided on the basis of religious demographics. This led to the creation of the sovereign states of the Pakistan (that later split into Pakistan and Bangladesh) and of India. The vast majority (over 95%) of Pakistan consider themselves Muslims whilst over 85% of India identifies as Hindu's. The partition led to a struggle between the newly constituted states of India and Pakistan and displaced up to 12.5 million people with estimates of loss of life varying from several hundred thousand to a million (most estimates of the numbers of people who crossed the boundaries between India and Pakistan in 1947 range between 10 and 12 million) and other atrocities.

The violent nature of the partition created an atmosphere of mutual hostility and suspicion between India and Pakistan that plagues their relationship to this day. A long-standing territorial dispute between India and Pakistan over the Kashmir region, the northwestern most region of South Asia, is known as the "Kashmir Conflict". India claims the entire state of Jammu and Kashmir and as of 2010, administers approximately 43% of the region, including most of Jammu, the Kashmir Valley, Ladakh, and the Siachen Glacier. India's claims are contested by Pakistan, which controls approximately 37% of Kashmir, namely Azad Kashmir or Pak Occupied Kashmir and the northern areas of Gilgit and Baltistan. The remaining part is claimed by China. At the time of partition, Jammu and Kashmir had a predominantly Muslim population, while having a Hindu ruler (Maharaja Hari Singh.) On partition Pakistan expected Kashmir to be annexed to it but it went to India. India has officially stated that it believes that Kashmir is an integral part of India, though the Prime Minister of India, Manmohan Singh, stated after the 2010 Kashmir Unrest that his government is willing to grant autonomy within the purview of Indian constitution to Kashmir if there is consensus on this issue. Pakistan officially maintains that Kashmir is the "jugular vein of Pakistan" and a currently disputed territory whose final status must be determined by the people of Kashmir. Certain Kashmiri independence groups believe that Kashmir should be independent of both India and Pakistan.

India and Pakistan have fought at least three wars over Kashmir, including the Indo-Pakistani Wars of 1947, 1965 and 1997. There was also a high-grade armed conflict in 1991 which the Pakistani forces occupied Indian-controlled Kargil range allegedly to provide cover for terrorists to cross over into Indian territory and were forced to retreat after suffering heavy losses.

Starting in the late 1980s the struggle has become increasingly more militant with the presence of Mujahideen insurgents and the Pakistani defeats adding to the bitterness. India alleges the pro-Kashmir insurgents are supported by Islamist terrorist groups from Pakistan-administered Kashmir and Afghanistan, fighting to make Jammu and Kashmir, a part of Pakistan. India claims Pakistan is supplying munitions to the terrorists and training them in Pakistan. These claims were bolstered by Osama bin Laden's 2002 'Letter to American People' wherein he stated that one of the reasons he was fighting America is because of its support of India on the Kashmir issue. American special forces were sent into Indian-administered Kashmir in 2002 to hunt for bin Laden following reports that he was being sheltered by the Kashmiri militant group.

Pakistan has often used proxy terrorists groups to achieve its foreign policy goal. The 2008 Mumbai attacks brought the Kashmir issue to light again. Twelve coordinated shooting and bombing attacks occurred across Mumbai at the hands of Islamist terrorists who were trained in and came from Pakistan. Ajmal Kasab, the only attacker who was captured alive, later confessed upon interrogation that the attacks were conducted with the support of Pakistan's ISI. The attacks killed 164 people and wounded at least 308. The following are the most significant groups in the region:

Lashkar-e-Tayyiba (LeT) - Pakistan/Kashmir

Lashkar e-Tayyiba (LeT), whose name translates to mean 'Army of the Pure', is one of the largest and most proficient of the Kashmiri-focused militant groups. LeT was founded in 1987 by Professor Hafiz Saeed as the militant wing of the Islamist organisation Jamat-ud-Dawa. Saeed was a respected ulama of the relatively small Ahl-e-Hadith movement based mainly in Pakistan that advocated an Islamic purification of society. Having gained military experience during the Afghan jihad, Saeed represented the ideal blend of religious authority and military expertise to lead a group of Islamic jihadists. The jihad espoused by Saeed and the LeT, and that advocated by Al-Qaeda should not however be taken as one and the same phenomenon. Where AQ seeks to wage war against a "Zionist-Crusader alliance", the Pakistan based LeT's struggle is against a "Hindu-Zionist-Crusader alliance". In this respect LeT attacks against the Indian government can be seen as dating back to the divisive policy adopted by colonisers. The purported objective of LeT campaigns is to create an Islamic state in South Asia and to liberate Muslims residing in Indian administered Kashmir.

The centres of LeT recruitment, training, and support are the Punjab province of Pakistan and Pakistan administered Kashmir. The primary focus of the organisation's operations is the Kashmir jihad, a campaign the LeT gives precedence over all other Islamic jihad's as a result of both its proximity and the high ratio of Indian occupation forces to population. However the LeT's quarrel with India runs far deeper than simply the contest for Kashmir, with the group in fact intending to reassert Muslim control over the entire subcontinent. This larger goal explains why LeT attacks have not been isolated to Indian targets in Kashmir, but have struck across India, including in 2001 on the Indian Parliament and the infamous Mumbai attacks of 2008.

The Mumbai attacks consisted of 12 bombings and shootings across the capital and claimed the lives of 164 people. Upon interrogation one of the attackers Ajmal Kasab admitted that the LeT had received support from Pakistan's Inter-Services Intelligence (ISI), raising the possibility that despite official condemnation of the group, the LeT may have acted as a proxy organisation for the Pakistani government and its aggressive foreign policy towards India. This possibility was confirmed by the 2011 testimony of David Healey, a US-Pakistani who had in a previous trial pleaded guilty to plotting the Mumbai attacks, as well as an aborted LeT attack against a Danish newspaper. As a witness in the trial of Tahawwur Rana, accused of providing financial support for the LeT attacks in Mumbai, Healey asserted that Pakistan's ISI had provided the group with both moral and military aid.

LeT funds are believed to be drawn from Pakistani and Kashmiri businessmen, as well as the Pakistani diaspora community residing in the Persian Gulf and the UK. Charities in particular have provided large amounts of money for the organisation, following the Kashmir earthquake of 2005 charity collections were made in Britain under the pretext of providing aid to the stricken Kashmiri community through alleged front organisations. While some of the money may have reached their official beneficiaries, in some areas the LeT were the first group to arrive with aid. It is feared that more than half of the £5 million collected was siphoned off to fund violent LeT operations. There also remains the distinct possibility that the Pakistani ISI may have provided financial support for some LeT operations.

The exact organisation size of the LeT is unknown; however it estimated by some sources that the group possesses several thousand members. Despite the nexus of LeT activity being focused in and around the Indian subcontinent, some members are known to have fought in Chechnya and in the Philippines during the 1990s. In 2009 the organisation declared that it had ceased its violent operations and sought a peaceful resolution to the dispute over the governance of Kashmir. Nevertheless LeT is still considered to be an active terrorist group with significant military capabilities.

Jaish-e-Mohammed (JEM) - Pakistan/Kashmir

Jaish-e-Mohammed was designated as a Foreign Terrorist Organisation on December 26, 2001, Jaish-e-Mohammed (JEM) is based in Pakistan. JEM was founded in early 2000 by Masood Azhar, a former senior leader of Harakat ul-Ansar, upon his release from prison in exchange for 155 hijacked Indian Airlines hostages in India. The group's aim is to annex Indian Kashmir and expel Coalition Forces from Afghanistan, and it has openly declared war against the US. Pakistan outlawed JEM in 2002. By 2003, JEM had splintered into Khuddam-ul-Islam (KUI), headed by Azhar, and Jamaat ul-Furqan (JUF), led by Abdul Jabbar, who was released from Pakistani custody in August 2004. Pakistan banned KUI and JUF in November 2003.

JEM continues to operate openly in parts of Pakistan despite the 2002 ban on its activities. Since Masood Azhar's 1999 release from Indian custody, JEM has conducted many fatal terrorist attacks in the region. JEM claimed responsibility for several suicide car bombings in Kashmir, including an October 2001 suicide attack on the Jammu and Kashmir legislative assembly building in Srinagar that killed more than 30 people.

The Indian government has publicly implicated JEM, along with Lashkar e-Tayyiba, for the December 2001 attack on the Indian Parliament that killed nine and injured 18. In 2002, Pakistani authorities arrested and convicted a JEM member for the abduction and murder of US journalist Daniel Pearl. Pakistani authorities suspect that JEM members may have been involved in the 2002 anti-Christian attacks in Islamabad, Murree, and Taxila that killed two Americans.

In December 2003, Pakistan implicated JEM members in the two assassination attempts against President Musharraf. In 2006, JEM claimed responsibility for a number of attacks, including the killing of several Indian police officials in the Indian-administered Kashmir capital of Srinagar. Indian police and JEM extremists continued to engage in firefights throughout 2008 and 2009. In March 2011, Indian security forces killed chief JEM commander Sajad Afghani and his bodyguard in Srinagar, Kashmir.

In anticipation of asset seizures by the Pakistani government, JEM withdrew funds from bank accounts and invested in legal businesses, such as commodity trading, real estate, and production of consumer goods. In addition, JEM collects funds through donation requests in magazines and pamphlets, sometimes using charitable causes to solicit donations.

Harakat-ul Jihad Islami (HUJI) - Pakistan/Kashmir

Harakat-ul Jihad Islami was designated as a US Foreign Terrorist Organisation on 6 August 2010, Harakat-ul Jihad Islami (HUJI) was founded in 1980 in Afghanistan to fight against the Soviet Union. Following the Soviet withdrawal from Afghanistan in 1989, the organisation re-focused its efforts on India.

HUJI seeks the annexation of Indian Kashmir and expulsion of Coalition Forces from Afghanistan. It also has supplied fighters for the Taliban in Afghanistan. In addition, some factions of HUJI espouse a more global agenda and conduct attacks in Pakistan against US targets as well. HUJI is composed of militant Pakistanis and veterans of the Soviet-Afghan war. HUJI has experienced a number of internal splits and a portion of the group aligned with Al-Qaeda in recent years, including training its members in AQ training camps. Mohammad Ilyas Kashmi, one of HUJI's top leaders who also served as an AQ military commander and strategist, was killed on 3 June 2011.

HUJI has been involved in a number of terrorist attacks in recent years. On 2 March 2006, a HUJI leader was the mastermind behind the suicide bombing of the US Consulate in Karachi, Pakistan, which killed four people, including US diplomat David Foy, and injured 48 others. HUJI was also responsible for terrorist attacks in India including the May 2007 Hyderabad mosque attack, which killed 16 and injured 40, and the March 2007 Varanasi attack, which killed 25 and injured 100. HUJI claimed credit for the September 7, 2011 bombing of the New Delhi High Court, which left at least 11 dead and an estimated 76 wounded. HUJI sent an e-mail to the press stating that the bomb was intended to force India to repeal a death sentence of a HUJI member.

Harakat ul-Mujahideen (HUM) - Pakistan/Kashmir

Harakat ul-Mujahideen was designated as a US Foreign Terrorist Organisation on 8 October 1997, Harakat ul-Mujahideen (HUM) seeks the annexation of Indian Kashmir and the expulsion of Coalition Forces in Afghanistan. Reportedly under pressure from the Government of Pakistan, HUM's long-time leader Fazlur Rehman Khalil stepped down and was replaced by Dr. Badr Munir as the head of HUM in January 2005.

Khalil has been linked to Al-Qaeda and bin Laden, and his signature was found on bin Laden's February 1998 fatwa calling for attacks on US and Western interests. HUM operated terrorist training camps in eastern Afghanistan until Coalition air strikes destroyed them in 2001. Khalil was detained by Pakistani authorities in mid-2004 and subsequently released in late December of the same year. In 2003, HUM began using the name Jamiat ul-Ansar (JUA). Pakistan banned JUA in November 2003. HUM has conducted a number of operations against Indian troops and civilian targets in Kashmir. It is linked to the Kashmiri militant group al-Faran, which kidnapped five Western tourists in Kashmir in July 1995. The five reportedly were killed later that year.

HUM was responsible for the hijacking of an Indian airliner in December 1999 that resulted in the release of Masood Azhar, an important leader in Jamiat ul-Ansar, who was imprisoned by India in 1994 and founded Jaish-e-Mohammed (JEM) after his release. Another for-

mer member of Harakat ul-Ansar, Ahmed Omar Sheik was also released by India as a result of the hijackings and was later convicted of the abduction and murder in 2002 of US journalist Daniel Pearl. HUM targets Indian security and civilian targets in Kashmir. In 2005, such attacks resulted in the deaths of 15 people. In November 2007, two Indian soldiers were killed in Kashmir while engaged in a firefight with a group of HUM militants. Indian police and army forces have engaged with HUM militants in the Kashmir region, killing a number of the organisation's leadership in April, October, and December 2008. In February 2009, Kishen Advani, leader of the Indian opposition Bharatiya Janata Party, received a death threat that was attributed to HUM.

HUM collects donations from wealthy and grassroots donors in Pakistan, Saudi Arabia, and other Gulf states. HUM's financial collection methods include soliciting donations in magazine ads and pamphlets.

Al-Umar Mujahideen (AuM) - Kashmir

Al Umar Mujahideen was formed in 1989 to liberate the Indian State of Jammu and Kashmir through an armed struggle and merge it with Pakistan. The group has had the support of Pakistan's Inter-Services Intelligence Agency since the 1980s, during the early years of terrorist violence in Jammu and Kashmir, when the ISI perceived the AuM as a key group. The group is thought to have around 700 members. The group has been involved in numerous attacks including a grenade attack on the office of the separatist Democratic Freedom Party (DFP) in Srinagar in 2002.

Dukhtaran-e-Millat - Kashmir

Dukhtaran-e-Millat (Daughters of the Nation or DeM) is a radical Islamist women's group formed in 1987 and known for its vigilante efforts to impose strict Islamic practice in Indian-administered Kashmir, as well as its aid to other Kashmiri separatist groups. DeM was created in 1987 by Asiya Andrabi, a firebrand leader described as both a radical Islamist and feminist. Initially the group was formed to help Kashmiri women gain rights conferred to them by Islam, but the group quickly morphed into a militant organisation. Leaving behind their original concerns for women's rights, the group is now a religious-separatist movement that believes Kashmir should be part of Pakistan, and that violent jihad is necessary to bring about change in the region and the Islamic world as a whole.

The group made headlines in 1992 after attacking several Kashmiri women who defied a DeM communiqué ordering all women to wear the burqa (women's clothing that covers the whole body from head to toe, including the eyes, which are hidden behind a mesh veil).

In 1993, Andrabi was arrested with her husband, a member of the Hizb-ul-Mujahideen (HuM) militant group. Charged with "anti-national" activities, Andrabi

spent a year in jail, reportedly with her infant son.

The group has been responsible for numerous acts of violence against any act or business they deem immoral. The group has beaten women for sitting with men, destroyed liquor stores, and raided brothels. In response to this violence, Andrabi was again arrested, but was later freed. In addition to serving as a "morality police," the group is still thought to be aiding and abetting militant groups in the region, thus pursuing the twin goals of Islamic puritanism and Kashmiri separatism.

DeM is widely suspected of gun-running, money laundering, providing shelter, and serving as couriers and spies for several Kashmiri outfits including HuM and Jamiat ul-Mujahideen (JuM).

Hizb ul-Mujahideen (HuM) - Kashmir

Hizb ul-Mujahideen (HM) is the largest Kashmiri militant group, and officially supports the liberation of Kashmir and its accession to Pakistan, although some members are pro-independence. The group is the militant wing of Pakistan's largest Islamic political party, the Jamaat-i-Islami. It primarily targets Indian security forces and politicians in Kashmir and has conducted operations jointly with other Kashmiri militants.

It reportedly operated in Afghanistan through the mid-1990s and trained alongside the Afghan Hizb-I-Islami Gulbuddin in Afghanistan until the Taliban takeover. The group is made up primarily of ethnic Kashmiris but with some foreign sources.

While Indian intelligence reports that it is responsible for only about 10 to 20% of all terrorist strikes, Pakistani reports estimate that it controls about 60% of terrorists operating in Kashmir. The group was originally called Al Badr but was quickly renamed Hizb-ul Mujahideen.

Balochistan Liberation Army - Balochistan

The Balochistan Liberation Army is a separatist militant group based in a mountainous region of Western Pakistan, thought to be 500 strong, has conducted a series of attacks targeting security personnel, civilians and journalists. Nawabzada Hyrbyair Marri (born 1968) the fifth son of Baloch nationalist leader Khair Bakhsh Marri, is the current leader of the group. Baloch tribe is a famed warrior tribe, fiercely protective of their customs and culture, and have been involved in a conflict with the Pakistan authorities since the 1970s.

India



India is the seventh-largest country by area, the second-most populous country with over 1.2 billion people, and the most populous democracy in the world. Bounded by the Indian Ocean on the south, the Arabian Sea on the south-west, and the Bay of Bengal on the south-east, it shares land borders with Pakistan to the west; China, Nepal, and Bhutan to the north-east; and Burma and Bangladesh to the east.

India is derived from Indus, which originates from the Old Persian word Hindu. The latter term stems from the Sanskrit word Sindhu, which was the historical local name for the Indus River. India is home to the ancient Indus Valley Civilisation and a region of historic trade routes and vast empires. The Indian subcontinent was identified with its commercial and cultural wealth for much of its long history. Four world religions - Hinduism, Buddhism, Jainism, and Sikhism - originated here. Starting in the early 18th century, India was gradually annexed by and brought under the administration of the British East India Company and administered directly by the United Kingdom from the mid-19th century. India became an independent nation in 1947 after a struggle for independence that was marked by non-violent resistance led by Mahatma Gandhi.

The partition of India was set forth in the Indian Independence Act 1947 and resulted in the dissolution of the British Indian Empire and the end of the British Raj. British India was largely divided on the basis of religious demographics. This led to the creation of the sovereign states of the Dominion of Pakistan (that later split into the Islamic Republic of Pakistan and the People's Republic of Bangladesh) and the Union of India (later Republic of India). The violent nature of the partition created an atmosphere of mutual hostility and suspicion between India and Pakistan that plagues their relationship to this day. For more details see the Kashmir and Jammu Conflict above in Pakistan.

India has officially stated that it believes that Kashmir is an integral part of India, though the Prime Minister of India, Manmohan Singh, stated after the 2010 Kashmir Unrest that his government is willing to grant autonomy within the purview of Indian constitution to Kashmir if there is consensus on this issue. Pakistan maintains that Kashmir is the "jugular vein of Pakistan" and a currently disputed territory whose final status must be determined by the people of Kashmir. Certain Kashmiri independence groups believe that Kashmir should be independent of both India and Pakistan.

India's rapidly growing economy has of course a formal but also an extensive informal economy and remittance system which with persistent corruption and strict currency controls contributing to its vulnerability to economic crimes, including fraud, cybercrime, identity theft, money laundering and terrorist financing. India's porous borders and location between heroin-producing countries in the Golden Triangle of Southeast Asia and Golden Crescent of Central Asia make it a frequent transit point for drug trafficking. Proceeds from Indian-based heroin traffickers is widely known to re-enter the country via bank accounts, the hawala system, and money transfer companies. High-level corruption both generates and conceals criminal proceeds. Illicit funds are often laundered through real estate, educational programmes, charities, and election campaigns. The most common money laundering methods include: opening multiple bank accounts, intermingling criminal proceeds with assets of legal origin, purchasing bank cheques with cash, and routing funds through complex legal structures. Transnational criminal organisations use offshore corporations and trade-based money laundering to disguise the criminal origin of funds. Companies use trade-based money laundering to evade capital controls. Tax avoidance and the proceeds of economic crimes are significant vulnerabilities but laundered funds are also derived from narcotics trafficking, trafficking in persons and illegal trade. Counterfeit Indian currency is also a significant problem. Criminal networks exchange high-quality counterfeit currency for genuine notes.

India remains a target of terrorist groups, both foreign and domestic. Several indigenous terrorist organisations coexist in various parts of the country; some are linked to external terrorist groups with global ambitions. Terrorist groups often use hawalas and currency smuggling to move funds from external sources to finance their activities in India. Indian authorities report they have seized drugs sold by India-based extremist elements to production and/or trafficking groups in neighboring countries.

Indian list of Designated Terrorist Organisations

India has listed the following as terrorist Organisations: Akhil Bharat Nepali Ekta Samaj (ABNES); Al Badr; Tri-pura Tiger Force; Al-Qaeda; Babbar Khalsa; Communist Party of India (Marxist-Leninist); Deendayal Anjuman; Dukhtaran-e-Millat (DEM); Harkat-ul-Mujahideen / Harkat-ul-Ansar / Harkat-ul-Jehad-e-Islami; Hizb-ul-Mujahideen / Hizb-ul-Mujahideen; Indian Mujahideen; International Sikh Youth Federation; Jaish-e-Mohammad; Tahrrik-e-Furqan; Jamiat-ul-Mujahideen; Jammu and Kashmir Islamic Front; Kanglei Yawol Kannu Lup (KYKL); Kangleipak Communist Party (KCP); Khalistan Zindabad Force aka Khalistan Commando Force; Lashkar-e-Taiba; Manipur People's Liberation Front (MLPF); Maoist Communist Centre (MCC); National Democratic Front of Bodoland (NDFB); National Liberation Front of Tripura; People's Revolutionary Party of Kangleipak (PREPAK); Tamil Nadu Liberation Army (TNLA); Tamil National Retrieval Troops (TNRT);

Liberation Tigers of Tamil Eelam (LTTE); United Liberation Front of Assam (ULFA); United National Liberation Front (UNLF); Students Islamic Movement of India (SIMI); and the Garo National Liberation Army (GNLA).

Indian Gangs

In India, organised crime is at its worst in the city of Mumbai. The first well-known organised gang to emerge was that of Varadharaj Mudaliar in the early sixties. His illegal activities included illicit liquor, gold smuggling, gambling, extortion and contract murders. Three other gangs emerged shortly thereafter namely, Haji Mastan, Yusuf Patel and Karim Lala. Haji Mastan and Yusuf Patel dealt in gold smuggling whereas Karim Lala operated in drugs. During the State of Emergency in 1975, a crackdown on the Mafia occurred and new gangs emerged, with Dawood Ibrahim, head of D-Company, the most successful among gangs came in conflict with the Pathan gangs led by dons Alamzeb and Amirzada Pathan. The Pathan gangs were ultimately destroyed to leave the field free for Dawood Ibrahim and D-Company. Other prominent members of D-Company include Chhota Shakeel, Tiger Memon and Abu Salem, who is now in the custody of Indian police after long drawn extradition negotiations. The other gangs of Mumbai operating in organised crime are those of Chhota Rajan (Drug Trafficking and Contract Killings), Arun Gawli (Contract Killings and Protection Money), Late Amar Naik (Protection Money) and Chhota Shakeel. Other forms of organised crime in India are kidnappings for ransom, gun running, illicit trafficking in women and children, money laundering. Organised crime exists in other cities as well, though not to the same extent as in Mumbai. Ahmedabad city is home to liquor smuggling because of prohibition policy (banning of liquor). There are several gangs operating in Delhi from the neighbouring State of Uttar Pradesh indulging in kidnapping for ransom. It is also reported that in recent years the ganglords of Mumbai have started using Delhi as a place for hiding and transit. Chhota Rajan group is strengthening its base in Delhi. The boom in construction activities in Bangalore city has also provided opportunity for organised crime. Builders are used for laundering money. The forcible vacation of old disputed buildings is a tactic used by Indian gangs and serves as a linkage between organised crime and construction trade. Recently, a prominent ex-official of the municipal body in charge of Mumbai, declared that he had identified 400 structures in Mumbai belonging to D-Company. There are also allegations of the movie industry being financed by organised crime lords and allegations that popular film stars performed at gang functions or at the behest of D-Company surface from time-to-time..

D-Company - Pakistan / India

D-Company is closely linked to a range of organised criminal and terrorist activities in South Asia, especially in Mumbai, India, and the Persian Gulf region and is led by Dawood Ibrahim. Several members of the

gang are on the "wanted list" of Interpol and Indian police. The organisation has a history of rivalry with the Mumbai police and other underworld dons such as Chhota Rajan, Ejaz Lakdawala who was arrested in Canada in 2004 and Arun Gawli. Ibrahim is said to have begun his career in Mumbai working for the Karim Lala gang exploiting the rapid expansion in the Bombay (now Mumbai) textiles industry to his advantage. He soon moved his residence to Dubai in the United Arab Emirates where he has business interests alongside India. Indian defence intelligence agencies believe that Ibrahim and his associates run a major criminal underworld operation and have huge stakes in the ship demolition industry in India and are using these operations for smuggling in arms, explosives and contraband into the country. Ibrahim is also believed to control much of the 'hawala' system in India. Ibrahim is widely believed to have organised and financed the March 1993 Bombay Bombings leading India to declare him "India's most wanted man". According to the US authorities, Ibrahim maintained close links with Al-Qaeda's bin Laden. In 2003 the US Department of Treasury designated Ibrahim as a terrorist. The US further pursued the matter before the UN in an attempt to freeze his assets around the world and crack down on his operations. In 2011, Indian intelligence agencies also linked D-Company with the 2G spectrum scandal. Ibrahim is thought to reside in Pakistan, receiving protection from the Pakistani Intelligence Services.

Students Islamic Movement of India

The Students Islamic Movement of India (SIMI), proscribed under the Unlawful Activities (Prevention) Act, 1967, is an Islamist fundamentalist organisation with a proclaimed agenda to convert non-followers to Islam by force and convert India into Dar-ul-Islam (land of Islam). The SIMI was formed at Aligarh in the State of Uttar Pradesh on April 25, 1977. Mohammad Ahmadullah Siddiqi, Professor of Journalism and Public Relations at the Western Illinois University Macomb, Illinois, was the founding President of the outfit. It originally emerged as a student wing of the Jamaat-e-Islami Hind (JIH). The alliance broke over ideological differences related to Palestine Liberation Organisation (PLO) leader Yasser Arafat's visit to India. JIH thereafter floated a new student wing, the Students Islamic Organisation (SIO). SIMI runs an active agenda of fundamentalist Islam, opposition of the secular and democratic values on which the nation state of India is founded and adoption of violence as means of achieving their goals. The group believes in Islamic indoctrination of youth and children through Madarassas, strong presence in Islamic universities and other centres of religious education and youth front organisations such as Shaheen Force, the outfit's wing for schoolchildren. It supports secession of Jammu and Kashmir and is believed to have close links with Inter-Services Intelligence of Pakistan. SIMI has aligned itself with bin Laden whom they regard as a 'true believer of Islam' and are opposed to western culture and thought. The group also allegedly has links with almost every terrorist outfit with Islamic

leanings, a secessionist ideology and connections to Pakistan. The Indian police alleges that SIMI has transformed into the very violent and active terrorist group, Indian Mujahideen (IM), though some analysts believe that IM is a militant branch of SIMI while others believe that the two groups are distinct although linked. IM has claimed responsibility for a number of serial bomb blasts in crowded bazaars and commercial areas in Jaipur, Mumbai, Pune and other cities.

Indian Mujahideen (IM) - India

The Indian Mujahideen was designated as a US Foreign Terrorist Organisation on 19 September 2011. An India-based terrorist group with significant links to Pakistan, IM has been responsible for dozens of bomb attacks throughout India since 2005, and has caused the deaths of hundreds of innocent civilians. IM maintains close ties to other US-designated terrorist entities including Pakistan-based Lashkar e-Tayyiba (LeT), Jaish-e-Mohammed (JEM), and Harakat ul-Jihad-i-Islami (HUJI). IM's stated goal is to carry out terrorist actions against non-Muslims in furtherance of its ultimate objective, an Islamic Caliphate across South Asia. IM's primary method of attack is multiple co-ordinated bombings in crowded areas against economic and civilian targets to maximise terror and casualties. In 2008, an IM attack in Delhi killed 30 people; that same year, IM was responsible for 16 synchronised bomb blasts in crowded urban centres and a local hospital in Ahmedabad that killed 38 and injured more than 100. IM also played a facilitative role in the 2008 Mumbai attack carried out by LeT that killed 163 people, including six Americans. In 2010, IM carried out the bombing of a popular German bakery in Pune, India, frequented by tourists, killing 17 and injuring over 60 people. In 2011, IM conducted multiple bombings killing dozens of innocent civilians and injuring hundreds more. On 25 May IM was suspected of an improvised explosive device (IED) attack in New Delhi. On 13 July, 25 civilians were killed and 137 wounded in an IED attack in Mumbai. On 7 September, 15 civilians were killed, and 91 others injured in a bombing in New Delhi.

Sikh Terrorism - India

Sikh terrorism is sponsored by expatriate and Indian Sikh groups who want to carve out an independent Sikh state called Khalistan (Land of the Pure) from Indian territory. Active groups include Babbar Khalsa, Azad Khalistan Babbar Khalsa Force, Khalistan Liberation Front, Khalistan Zindabad Force and Khalistan Commando Force. Many of these groups operate under umbrella organisations, the most significant of which is the Second Panthic Committee. Sikh attacks in India are mounted against Indian officials and facilities, other Sikhs, and Hindus; they include assassinations, bombings, and kidnappings. These attacks have dropped markedly since 1992, as Indian security forces have killed or captured a host of senior Sikh militant leaders. Total civilian deaths in Punjab have declined more than 95% since more than 3,300 civilians died in 1991. The drop results largely from Indian Army, paramilitary, and

police successes against extremist groups. Sikh militant cells are active internationally and extremists gather funds from overseas Sikh communities. Sikh expatriates have formed a variety of international organisations that lobby for the Sikh cause overseas International Sikh Federation.

Babbar Khalsa International - India

Babbar Khalsa (BKI) is a Khalistani militant armed organisation based in India, it is considered a terrorist organisation by the Indian, US, Canadian and UK Governments. Despite setbacks incurred in the early 1990s following government action, BKI is still active.

Deendar Anjuman - South West India

Deendar Anjuman (DA) ("The Religious Association") is a Sufi Islamic sect formed in 1924 in the South West Indian State of Karnataka, whose capital and largest city is Bangalore, who came into prominence in the aftermath of 13 bomb explosions at various places of worship across the states of Andhra Pradesh, Goa and Karnataka in 2000. The group was proscribed in India in 2000. The DA perceives Islam as the only true global religion and regards Prophet Mohammed as the final prophet and uniquely, the sect interprets Islam as the logical conclusion of the spiritual beliefs of all 'true Hindus' and it also aims to convert India into an Islamic state. The group is alleged to be close to the Pakistani Inter Services Intelligence (ISI) and other Islamic fundamentalist groups in Pakistan and Saudi Arabia. Currently, it is reported to have established 150 branches comprising approximately 15,000 followers in India.

North Eastern India

India's North Eastern "Seven Sisters" region, an area made up of seven small northeastern states, has seen the emergence of several separatist armed groups seeking secession from the Federal Union of India. The different ethnic and cultural heritage of these states, late colonisation and unification with the rest of India in 19th century and their relative geographical isolation from the rest of India, has provided the separatist groups with a popular cause to canvass. These groups, with overlapping objectives and agreement over use of violence for achieving them, yet have significant differences in terms of ideology and leadership. The troubled border with China and porous borders with Bangladesh and Myanmar together with these countries' apparent policy of destabilizing the region, has provided fertile grounds for the growth of secessionist groups.

Most of these groups also have linkages with another hostile neighbour of India, Pakistan. The activities of most of these groups are localized in relatively small geographical areas and funded through criminal and unlawful activities. Many of these groups have targeted civilians besides the armed forces and police authorities and attack perceived outsiders, i.e. people from rest of India, living in the north eastern region. The Indian

Government has striven to meet the political aspirations of the diverse ethnic groups inhabiting the beautiful hills of Eastern Himalayas and valleys of Brahmaputra by carving out additional states and giving statehood to erstwhile union territories which has prompted a number of self-styled revolutionaries to join mainstream politics and governance. The terrorist outfits of North Eastern India are fairly unstable and frequently have in-fighting resulting in the formation of splinter groups. This constant splitting and reformation also makes them relatively difficult to track. The larger of these groups are discussed below.

Kanglei Yawol Kanna Lup - Manipur

The Kanglei Yawol Kanna Lup (KYKL) is an ethnic Meitei group based in Manipur, India. It is not a secessionist group but aims at strengthening the ethnic identity of the Meitei people and uniting the 'seven sister' states in the north eastern India. Ironically, it is formed from the dissenting factions of UNLF, PREPAK and Kangleipak Communist Party (KCP) 1994 and has carried out campaigns against other terrorist outfits. The group is infamous for its violent vigilantism and decrees aimed at "rebuilding Manipuri society" by "cleansing" it of immoral activities. Its terror activities are aimed at teachers, journalists, and HIV-positive innocents besides allegedly corrupt politicians, drug dealers and prostitutes. The group has issued decrees banning Hindi films, women wearing pants, and newspapers using Hindi script. The group claims that its objective is to cleanse Manipur of unwanted elements and moral corruption. KYKL funds its activities primarily through extortion that it collects jointly with the Nagaland-based National Socialist Council of Nagaland-Isak Muivah (NSCN-IM).

People's Liberation Front (PLA) - Manipur

The People's Liberation Army (PLA) was founded by N. Bisheshwar Singh on 25 September 1978. It is a separatist armed revolutionary group fighting for an independent socialist state of Manipur. It is allegedly the first organisation from Manipur to have been trained by the China's People Liberation Army at Lhasa in the 1980s National Socialist Council of Nagaland (NSCN) at its headquarters in north Myanmar during the 1980s.

The PLA aims to organise a revolutionary front covering the entire Northeast and unite all ethnic groups, including the Meiteis, Nagas and Kukis, to liberate Manipur. PLA, though a Meiti outfit, claims itself to be a trans-tribal organisation seeking to lead the non-Meiteis as well. Since its founding, it has been waging guerrilla warfare against the Indian Armed Forces and has targeted the Indian Army, Paramilitary Forces and the State Police Force. The organisation has an estimated strength of some 3800 as on 2008. PLA activists are equipped with sophisticated arms. The group has also been reportedly involved in widespread extortion operations. PLA is also a member of the Manipur Peoples Liberation Front, an umbrella organisation of separatist organisations of Manipur namely UNLF and PREPAK.

It has a government-in-exile in Bangladesh where the PLA has set up a number of bases in the Sylhet district. Two camps in Myanmar and five camps in Bangladesh are currently known to exist.

Revolutionary People's Front of Manipur

The Revolutionary People's Front (RPF) is the political wing of the People's Liberation Army (PLA), a militant group active in the northeastern Indian state of Manipur. RPF is essentially a government-in-exile based in Bangladesh. The group is well-organised, and includes departments for finances, publicity, and social welfare. Together, the RPF and the PLA are fighting to free Manipur from Indian 'colonial occupation.' Manipur was annexed by India, illegally according to the RPF, on October 15, 1949 and is one of the seven northeastern states (the 'Seven Sisters'). The 'Seven Sisters' are characterized by armed insurrections, ethnic and tribal tensions, and poor economic conditions. Although the RPF is a predominantly ethnic Meitei tribal group, it seeks to unite all ethnic and tribal groups in Manipur in order to liberate the territory.

Peoples Revolutionary Party of Kangleipak - Manipur

The People's Revolutionary Party of Kangleipak (PREPAK) was formed under the leadership of R.K. Tulachandra on October 9, 1977. The stated aim of PREPAK is to establish an independent state of Manipur for the ethnic Meitei people by ousting those who are considered outsiders to the valley of Manipur. It is believed to be trained variously by the National Socialist Council of Nagaland-Isak Muivah (NSCN-IM), the Kachin Independent Army (KIA) of Myanmar and has links with Pakistan's ISI. Like PLA and United National Liberation Front (UNLF), it is believed to have camps in Bangladesh and operates primarily in Manipur with occasional forays in neighbouring areas of Tripura and Nagaland. The group is armed with sophisticated weapons and has a history of targeting non-ethnic Meitei civilians, whom they consider as "outsiders" to the state, in the Manipur region along with government security forces, through bombings and small arms assaults. It is believed to indulge in extortion for financing its activities. The group remains active, though with limited influence and confined to a limited geographical area.

United National Liberation Front - Manipur

The United National Liberation Front (UNLF), the oldest Meitei insurgent group in Manipur, was formed as a non-violent organisation under the leadership of Areambam Samrendra Singh on 24 November 1964, dedicated to creating an independent political state and a socialist society. In 1990, the group publicly announced that they will take the course of armed struggle to achieve their goal of an independent Manipur. The group formed the Manipur People's Army (MPA) as an armed wing, and since that time, the UNLF has launched numerous attacks against Indian Army and se-

curity personnel besides fighting with other secessionist groups in Manipur, including Kanglei Yawol Kanna Lup and the National Socialist Council of Nagaland-Isak Muivah. During the 1990s the UNLF also took vigilante action against alcoholism, drug abuse, gambling, and other crime to undermine the executive and judiciary framework. The group has training camps in Myanmar and Bangladesh and finances its terror activities primarily by extortion, gun-running, and smuggling. UNLF is part of the tri-partite alliance of the Manipur Peoples Liberation Front together with PLA and PREPAK. The group continues to attack Indian security forces and participates in sporadic violence against rival insurgent groups over both ideological and ethnic issues and is considered the most significant terror threat in North Eastern parts of India.

United Liberation Front of Assom - Assam

United Liberation Front of Assam (ULFA) was formed on April 7, 1979, to establish a "sovereign socialist Assam" through an armed struggle. While ULFA was formed in 1979, the group did not commence significant activities until 1986. ULFA reportedly established camps along the Indo-Bhutan border in early 1990s and developed links with officers of Royal Bhutan Army and has allegedly been trained by the Inter Services Intelligence of Pakistan and Directorate General of Field Intelligence of Bangladesh. Links to China and Myanmar have been suggested as have connections to the Liberation Tigers of Tamil Eelam (LTTE) and the Afghan Mujahideen. ULFA allegedly also joined hands with terrorist outfits across North Eastern India and in Myanmar, with the Chin National Front supplying them with arms from Thailand. Claims of several commercial activities undertaken in Bangladesh for laundering money as well as drug trafficking have been made against Pares Baruah, one of the founders of ULFA. In the early 1990s, ULFA launched an aggressive campaign of terror attacks including holding 14 people for ransom in July 1991, an unsuccessful assassination attempt on Chief Minister Prafulla Kumar Mahanta in 1997, assassination of local minister Nagen Sharma in 2000, explosion killing school children in August 15, 2004 and killing of 62 migrant workers in 2007 in a series of attacks. On 5 February 2011, ULFA split in two parts Anti-Talks faction of ULFA ("ULFA ATF") led by Pares Baruah and Abhijit Barman and Pro-Talks faction of ULFA ("ULFA PTF") led by Arabinda Rajkhowa. A tripartite agreement for Suspension of Operations was signed by the Government of India, the State Government of Assam and the ULFA PTF on 3 September 2011. The ULFA PTF has since continued to engage in talks with Government of India.

ULFA ATF, which has an estimated strength of 150-250 militants, continues to recruit and train cadre and news reports suggest that it has camps in Myanmar, Garo hills of Meghalaya and Tirap and Changlang Districts of Arunachal Pradesh and Mon District of Nagaland as well as three camps in Bangladesh. The ULFA ATF continues to maintain linkages with other militant for-

mations in North Eastern parts of India and Myanmar and continues to enjoy the support of the Inter Services Intelligence of Pakistan.

National Democratic Front of Bodoland - Bodoland

Bodo Security Force (BdSF), formed on 3 October 1986 under the leadership of Ranjan Daimary, was in 1993 the National Democratic Front of Bodoland (NDFB) on 25 November 1994. The separatist outfit, active in the north eastern region of India, in particular north and north-west of the river Brahmaputra in Assam and areas close to the Assam-Meghalaya border, has been waging an armed campaign for a "sovereign Boroland" and "self-determination for the Bodos. The outfit has bases allegedly in Bangladesh, Myanmar and Bhutan and was very active in the 1990s.

Several acts of terror have been attributed to NDFB including 12 December 1992 attack on the 7th Assam Police Battalion headquarters at Choraikhola in Kokrajhar district and the nine serial blasts triggered by the outfit in Guwahati, Kokrajhar, Bongaigaon and Barpeta Road which resulted in high civilian casualties. It was alleged that NDFB, along with the ULFA, on various occasions was found to be channelling its funds through the "Bhutanese diplomatic bag" to their leaders based in Southeast Asian capitals. In December 2003, the government of Bhutan and the Indian Army launched joint operations to destroy these terrorist camps operated in Bhutanese territory by ULFA and NDFB. After the operations, which significantly undermined the strength of the outfit, the NDFB, on 8 October 2004, announced a six-month long unilateral ceasefire with effect from 15 October. Subsequently, a tripartite agreement between the Government of India, State Government of Assam and NDFB was signed on 25 May 2005 in New Delhi which has been extended repeatedly. The activities of NDFB had fallen significantly since the ceasefire. However, the recent formation of a new state in South India has led to the group raising its demand with renewed vigour. The Government of India has indicated that they would be willing to initiate negotiations for a tripartite permanent peace accord. As a first step, Daimary, who was handed over to India by Bangladesh on 1 May 2010, was granted conditional bail on 24 June 2013 in all of the 13 cases pending against him.

National Liberation Front of Tripura - Tripura

The National Liberation Front of Tripura (NLFT) was formed on 12 March 1989, with Dhananjoy Reang (former Vice-President of the Tripura National Volunteers) as its 'Chairman'. The stated purpose of NLFT is to secede from India and establish an independent Tripura state, through an armed struggle. The NLFT manifesto says that they want to expand what they describe as the kingdom of God and Christ in Tripura. NLFT is constantly in flux and has given rise to several splinter groups. In 2001, NLFT split into two main factions, one led by Nayanbasi Jamatiya and the other by Biswamohan Debbarma. According to confiscated records of NLFT, the split was caused by internal bicker-

ing among senior leaders, misappropriation of funds by certain senior NLFT members, and disagreement over the forcible conversion of NLFT members to Christianity. According to at least one report, approximately 90% of senior NLFT members are Christians. Despite the internal fighting and regardless of future splintering of the NLFT, the group remains an active terrorist threat in the Tripura state of India. Indian Government officials have accused the Baptist Church of Tripura of supporting this violent campaign by providing funding and arms for the group. In April 2000, Nagmanlal Halam, secretary of the Noapara Baptist Church in Tripura, was caught providing 50 gelatin sticks, 5kgs of potassium and 2kgs of sulphur and other ingredients for making explosives to the group. The NLFT operates from camps based in Bangladesh and along the Indian-Bangladesh border. NLFT has further links with the Inter Services Intelligence Agency (ISI), Pakistan's external intelligence agency and its counterpart in Bangladesh, the Directorate General of Forces Intelligence (DGFI). During 1997-98, NLFT leaders are reported to have visited Pakistan to receive training and arms from the ISI. The NLFT is currently proscribed as a terrorist organisation in India.

Garo National Liberation Army - Garoland

The Garo National Liberation Army (GNLA) was formed in 2009 and is fighting for a 'sovereign Garoland' in North Eastern India in the Western areas of Meghalaya. Since its formation, from local police and security units, the GNLA has been involved in killing, abduction, extortion, bomb blasts and attacks on Indian Security Forces. The GNLA has forged close operational links with other North-East-based militant groups like the United Liberation Front of Assam (ULFA) and the NDFB. It also has links with the National Socialist Council of Nagaland-Isak-Muivah (NSCN-IM). The outfit has also forged an alliance with the Bangladesh-based militant group, A'chik Special Dragon Party, which operates along the India-Bangladesh border in the western part of Meghalaya. It is believed to have around 70 active members. The Government of India, which initially dismissed the GNLA as a "bunch of criminals", invited in 2010, the group for talks to "facilitate their surrender", without so far any success.

Hynniewtrep National Liberation Council (HNLC) - Meghalaya / Garoland

The Hynniewtrep National Liberation Council (HNLC) was formed in 1992 as a militant tribal outfit seeking to transform Meghalaya in India as a province exclusively for the Khasi tribe and free it from 'domination' by the Garo tribe and to fight against the presence of 'outsiders'. The HNLC was proscribed as a terrorist organisation by the Government of India in 2000. The top leadership of the group is based in the Bangladeshi capital Dhaka, with many HNLC camps also located in Bangladesh. The HNLC is closely linked with the National Socialist Council of Nagaland and the National Liberation Front of Tripura.

Achik National Volunteer Council (ANVC) - Garoland

The Achik National Volunteer Council (ANVC) was formed in 1995 to carve out a homeland called 'Achik Land' in the areas of Garo Hills. The proposed 'Achik Land' comprises the present districts of Garo Hills in Meghalaya and a large district of Assam, which is home to a 'Garo majority' in these areas. Whilst the group was proscribed in 2000, it signed a ceasefire agreement with the Government of India in 2004.

Tamil Nadu Liberation Army - Tamil Nadu

In the early 1980s, a number of separatist groups emerged in Tamil Nadu. These groups were active during the period when the Indian Peacekeeping Force (IPKF) was sent to Sri Lanka and pro-Liberation Tigers of Tamil Eelam (LTTE) sentiments were running high among a section of people in the State. The groups laid claim to a Greater Tamil Nadu independent of India and comprising not just the Indian state for Tamil Nadu and Karnataka but diverse regions such as Sri Lanka and the Maldives, based on shared Dravidian language and culture. These groups had linkages with the Liberation Tigers of Tamil Eelam, the armed rebel group in Sri Lanka which was recently defeated by the Sri Lankan army in a long and bitter civil war.

These groups were also linked to local criminals such as the notorious sandalwood smuggler, Veerappan who was killed in 2004 after years of being chased by the police force of three of the southern states of India. Tamil Nadu Liberation Army (TNLA), one such group, became active in Tamil Nadu in this period. Pulavar Kaliyaperumal, a former school teacher and a left-wing Naxalite extremist, initiated a debate on Tamil nationalism leading to a split in the all-India unit of the Communist Party of India-Marxist-Leninist (CPI-ML). The separatist faction formed Tamil Nadu Communist Party-Marxist-Leninist (TNCP-ML) in 1984-85 with the goal of achieving an independent Tamil home-land through armed struggle. The TNCP-ML's armed wing was named TNLA. Sundaram headed the TNCP-ML and Thamizharasan, an engineering student from Ponparappi village, headed the TNLA. TNLA engaged in bomb blasts, murders and even bank robbery.

India proscribed the TNLA, however, official sources have indicated that after the proscription, the TNLA operated under a new name. "Tamizhar Vidhuthalai Iyakkam".

Tamil National Retrieval Troops - Tamil Nadu

Another group with similar aims and connections is the Tamil National Retrieval Troops ("TNRT"). It is a small outfit and is believed to be functioning since the late eighties in the southern Indian State of Tamil Nadu, though its exact date of founding is not known. The TNRT was founded by Ravi alias P. Ravichandran. He was an accused in the 1990-murder, in Chennai, of Eelam People's Revolutionary Liberation Front (EPRLF)

general secretary Padmanabha and the 1991 assassination in Sripurambadur of former Indian Prime Minister Rajiv Gandhi. Ravi was sentenced to life in prison in 1999 in connection with the Rajiv Gandhi assassination case. Since Ravi's imprisonment, it is not known who has been providing leadership to TNRT cadres. It has been proscribed under the Prevention of Terrorism Act (POTA), 2002. Several other groups in Tamil Nadu, such as Thamizh Thesi Pothuvudai Katchi (TTPK), Tamil National Liberation Movement, propagate the idea of a separate and independent Tamil nation. However these claim to be believers of the democratic process and do not advocate violence.

Communist Party of India (CPI-Maoist)/The Maoist Communist Centre of India (MCC)

The MCC came into existence, in an earlier version in 1969, as Dakshin Desh, which refused to join in with the mergers at the time leading to the creation of the Communist Party of India (Marxist-Leninist). Dakshin Desh was renamed in 1975 as the Maoist Communist Centre. Like other left wing extremist groups, the purported objective of the MCC is to establish a 'people's government' through 'people's war'. It traces its ideology to the Chinese Communist leader Mao Zedong's teachings of organised peasant insurrection. The MCC was mostly active in areas of West Bengal with attempts also to operate in parts of Uttar Pradesh. In September 2004, the MCC merged with the People's War Group (another left-wing extremist group) to form the Communist Party of India-Maoist (CPI-Maoist), whereupon the MCC ceased to exist. The CPI-Maoist's current goal is to establish a "Compact Revolutionary Zone," an area of control that would extend from the Nepalese border to Andhra Pradesh in the south. Eventually this zone would be converted into an independent communist state. The Indian government is vehemently opposed to any territorial concessions to the group.

Bangladesh

The name Bangladesh means "Country of Bengal" and is an independent country, which together with the neighbouring Indian state of West Bengal, makes up the region of Bengal. The borders of modern Bangladesh took shape during the Partition of Bengal and British India in 1947, when the region became first East Pakistan, being the eastern wing of the newly formed state of Pakistan and later in 1971 to full independence as Bangladesh. Bangladesh is a parliamentary republic with a population of more than 160 million people, being one of the world's most densely populated countries. The Bengalis form the country's predominant ethnic group, with almost 90% following Islam. After a series of military coups and corrupt governments, the country returned to fully democratic rule only in December 2008 with the election of Prime Minister Sheikh Hasina as head of the Awami League and the party that fought for original independence.

Bangladesh's geographic location, including its seaports and long porous borders with India and Burma, make it a transhipment point for drugs produced in both the "golden triangle" of Southeast Asia and "golden crescent" of Central Asia. In addition to drug trafficking, corruption, fraud, counterfeit money, and trafficking in persons are the principle sources of illicit proceeds. Bangladesh is also vulnerable to terrorist financing, including funding that flows through the hawala/hundi system and by cash courier. The Bangladesh-based terrorist organisation's Jamaat ul-Mujahideen Bangladesh and Harakat ul-Jihad-i-Islami are looking to establish Islamic law and strict adherence in the country and are co-operating with Pakistani and Afghan groups with similar aims. Black market money exchanges remain popular because of the non-convertibility of the local currency and scrutiny of foreign currency transactions made through official channels. Alternative remittance systems are also used to avoid taxes and customs duties. Additional terrorism financing vulnerabilities exist, especially concerning the use of non-governmental organisations (NGOs), charities, counterfeiting, and loosely-regulated private banks.

Jamaat-ul-Mujahideen - Bangladesh

Jamaat-ul Mujahideen Bangladesh (JMB) is an Islamist organisation operating in Bangladesh. It was founded in 1998 in Palampur in Dhaka division by Abdur Rahman and gained public prominence in 2001 when bombs and documents detailing the activities of the organisation were discovered in Parbatipur in Dinajpur district.

The organisation was officially banned by the government of Bangladesh in February 2005. The stated aim of JMB is to advocate fundamentalist Islam, Islamic law and liberating Muslims of the influence of 'anti-Islam forces' and practices. They are proclaimed anti-west, US and Britain which they believe are occupying Muslim lands. They are opposed to popular arts such as music and cinema and view NGOs as creatures of western governments. They are also against women's emancipation and integration in the society. JMB aims at establishing the rule of Islam in Bangladesh through an armed struggle. Some reports suggest that it is the youth front of the Al Mujahideen, an organisation allegedly formed in the mid-1990s but whose existence is still ambiguous, whereas others indicate that the JMB is another name for the vigilante Islamist group the Jagrata Muslim Janata Bangladesh (JMJB). Maulana Saidur Rahman is known to be currently heading the JMB.

JMB has run a campaign of terror in North Bangladesh with terror attacks in public places. Following the ban by Bangladesh government, the group carried out a massive attack by detonating detonated 500 bombs at 300 locations throughout Bangladesh in August 2005 attacking in 63 of the 64 Districts in the country.

The JMB allegedly receives funding from individual donors in countries like Kuwait, the UAE, Bahrain, Pakistan, Saudi Arabia and Libya. Several international

NGOs such as the Kuwait-based Revival of Islamic Heritage and Doulatul Kuwait, UAE-based Al Fuzaira, Khairul Ansar Al Khairia, Bahrain-based Doulatul Bahrain and the Saudi Arabia-based Al Haramain Islamic Institute have also said to have provided funding to the outfit, though any links to terrorism have been denied. The JMB and its leaders are reported to have invested in a large number of shrimp farms and cold storages in the south-western region of Bangladesh. The outfit is also alleged to be involved in money laundering activities, collecting illegal taxes and extortion to fund its terror activities and channeling funds through illegal channels known as Hundi. The outfit remains an active threat in Bangladesh.

Harakat ul-Jihad-i-Islami - Bangladesh

Designated as a US Foreign Terrorist Organisation on 5 March 2008, Harakat ul-Jihad-i-Islami/Bangladesh (HUJI-B) was formed in April 1992 by a group of former Bangladeshi Afghan veterans to establish Islamic rule in Bangladesh.

In October 2005, Bangladeshi authorities banned the group, HUJI-B has connections to Pakistani militant groups such as Lashkar-e-Tayyiba (LeT) and the Indian Mujahideen (IM), which advocate similar objectives. The leaders of HUJI-B signed the February 1998 fatwa sponsored by Al-Qaeda and bin Laden that declared American civilians legitimate targets. In December 2008, three HUJI-B members were convicted for the May 2004 grenade attack that wounded the British High Commissioner in Sylhet, Bangladesh. In 2011 Bangladeshi authorities formally charged multiple suspects, including HUJI-B leader Mufri Abdul Hannan, with the killing of former Finance Minister Shah AMS Kibria of Awami League (AL) in a grenade attack on 27 January 2005. Bangladeshi police also arrested many top HUJI-B leaders in 2011, including Amir Rahmatullah (aka Sheikh Farid) in April, and chief Moulana Yahiya in August. Bangladeshi police recovered arms, explosives and bomb making materials following the arrest of HUJI-B operative Abdul Alim in May. HUJI-B leaders claim that up to 400 of its members are Afghan war veterans, but its total membership is unknown.

The group operates primarily in Bangladesh and India. HUJI-B trains and has network of madrassas in Bangladesh. HUJI-B funding comes from a variety of sources. Several international Islamic non-governmental organisations may have funneled money to HUJI-B and other Bangladeshi militant groups.

Nepal

Nepal as a population of approximately 27 million, is located in the Himalayas and bordered to the north by China, (the Tibetan autonomous region) and to the south, east, and west by India. The mountainous north of Nepal has eight of the world's ten tallest mountains,

including Mount Everest. It is also the birthplace of the Buddha, though Hinduism is practiced by about 80% of Nepalis.

In 1951, the Nepali monarch ended the century-old system of hereditary rule and instituted a cabinet system of government.

An insurgency led by Maoist extremists broke out in 1996. The ensuing 10-year civil war between the Communist Party of Nepal (Maoist) (now known as the Unified Communist Party of Nepal (Maoist)) and government forces culminated in a 2006 peace accord. The ensuing elections in 2008 overwhelmingly favored the abolition of the monarchy and the establishment of a federal multiparty representative democratic republic.

In recent developments, political parties of Nepal have agreed on forming an interim election government, (with coalition governments including the Unified Communist Party) under the leadership of Chief Justice Khil Raj Regmi who is charged with holding Constituent Assembly elections by December 2013.

Government corruption, poorly regulated trade, weak financial sector regulation, and a large informal economy make the country vulnerable to money laundering and terrorist finance. Although Nepal is neither a significant producer of, nor a major transit route for narcotic drugs, hashish, heroin, and domestically produced cannabis and opium are trafficked to and through Nepal every year, en route from South East Asia to the West.

Its relatively porous borders with India and China are used to conceal trafficking in drugs and human beings. The major sources of laundered proceeds stem from tax evasion, corruption, counterfeit currency, smuggling, and invoice manipulation.

The Communist Party of Nepal-Maoist - Nepal

The CPN-M's strategy and tactics are based on traditional Maoist guerrilla war principles. As part of its struggle against the current regime, the Maoists have targeted Nepalese parliamentarians, the Prime Minister, government ministries, and a number of educational institutions. International targets have occasionally been hit as well, largely in an effort to isolate the government.

Two US embassy guards were assassinated by the Maoists in 2002, allegedly for anti-Maoist spying activities. Further attacks against diplomatic targets have been threatened in CPN-M press releases. Foreign commercial groups are also targets for the Maoists, as they demonstrated in three attacks on Coca-Cola facilities and one attack on a Pepsi-Cola truck.

Despite a massive effort from the Royal Nepalese Army (at the behest of then King Gyanendra) to crackdown on the CPN-M, the group enjoys widespread support and is believed to control an estimated 70% of the Nepalese countryside. The CPN-M have an estimated strength of 10,000-20,000 armed members with an

arsenal that has increased in both size and sophistication in recent years. In addition to receiving funds and support from expatriate Nepalese living in India, the group funds its operations through extortion, "taxation" and bank robberies.

The group maintains bases in India as well as Nepal and enjoys support from many Indian insurgent groups, most notably the [United Liberation Front of Assam](#) and the [Communist Party of India-Maoist \(CPN-M\)](#).

In February 2005, ostensibly due to his inability to crush the rebels, King Gyanendra issued a state of emergency and dismissed parliament. Although this move was done purportedly to defeat the CPN-M, Gyanendra's power-grab seems to have only strengthened the rebel's position. Widespread opposition to the King's move amongst the Nepalese people has lent credence to the rebel movement and has served to improve ties between the CPN-M and other legitimate political parties.

In April 2006, facing massive protests, King Gyanendra gave up power and announced that parliament would re-assemble. In November 2006, CPN-M and the Nepalese political establishment reached a peace deal which would see the rebels disarming under UN supervision and joining the Nepalese parliament as the second largest party. The peace agreement has been hailed as "historic" and a "landmark" for ending violence in Nepal.¹⁸

Whilst the CPN-M was designated in 2003 by the US as a global terrorist entity, it was removed from the US list of designated global terrorist groups in 2011.

Akhil Bharat Nepali Ekta Samaj - Nepal

Akhil Bharat Nepali Ekta Samaj (ABNES) was formed to form unity and provide support among immigrant Nepalese residing in India. However, ABNES gradually became involved in terrorism and began to function as a front for the Maoist insurgents of Nepal. It is also believed that the organisation is working for the proliferation of a greater Nepal idea. ABNES has established an extensive network all over India. It has a strong base in northern Bengal and is active in Northeast India, Uttar Pradesh and Bihar, in areas inhabited by ethnic Nepalese, and in stretches bordering Nepal. ABNES have ties with left-wing extremists of the People's War Group (PWG) and [Maoist Communist Centre \(MCC\)](#), who have strong ties with the Maoist insurgents.

The PWG, MCC and the Maoist insurgents are members of a left-wing extremist coalition, Coordinating Committee of Maoist Parties and Organisations in South Asia (CCOMPOSA), which was founded in mid-2001. A youth organisation known as the Akhil Bharatiya Nepali Vidyarthi Sangh, is closely linked to the activities of ABNES. ABNES was proscribed in 2002.

Sri Lanka

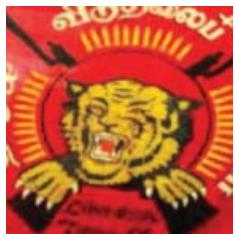
Sri Lanka, is an island country in the northern Indian Ocean off the southern coast of the Indian subcontinent in South Asia and known until 1972 as Ceylon. Sri Lanka is known as "the Pearl of the Indian Ocean" because of its natural beauty. Sri Lanka has also been called "the teardrop of India" because of its shape and location, and "the nation of smiling people". The island contains tropical forests and diverse landscapes with high biodiversity. Sri Lanka is a diverse country, home to many religions, ethnicities and languages. It is the land of the Sinhalese, Sri Lankan Tamils, Moors, Indian Tamils, Burghers, Malays, Kaffirs and the aboriginal Vedda.

The first Sinhalese arrived in Sri Lanka late in the 6th century B.C., from northern India. And in the 14th century, a south Indian dynasty established a Tamil kingdom in northern Sri Lanka. The island came under British rule by 1815, becoming known as Ceylon, later achieving independence in 1948 and changing its name to Sri Lanka in 1972. The country's recent history has been marred by a thirty-year civil war between the government forces representing the Sinhalese majority and the [Tamil Tigers \(LTTE\)](#) representing the Tamil minority in the North of the Island, which decisively but controversially ended in a military victory in 2009 by the government.

President Rajapaksa attained the Presidency in 2005 and was re-elected in 2010 to a second term. Allegations of war crimes have surfaced by WikiLeaks who made public secret US cables from 2009–10, stating that American diplomats believed that President Rajapaksa was responsible for the massacres of Tamil civilians and captured LTTE fighters at the end of the war with the LTTE. The cable also states the responsibility for many of the alleged crimes rests with the country's senior civilian and military leadership, including President Rajapaksa, his brothers and Former Army Chief General Fonseka. In April 2011, Ban Ki-moon published a report by a UN-appointed panel of experts, which concluded that as many as 40,000 people were killed in the final weeks of the war between the [Tamil Tigers](#) and government forces. For their part, Rajapaksa and his government have denied all allegations of war crimes. Sri Lanka is not an important regional financial center nor a preferred center for money laundering. However, there is corruption in government, experience with terrorism, tax evasion, and a large informal economy make the country vulnerable to money laundering and terrorist finance. Sri Lanka is primarily a source country for men, women, and children subjected to forced labour and sex trafficking, including in Saudi Arabia, Kuwait, Qatar, the United Arab Emirates, Jordan, Bahrain, Lebanon, Iraq, Afghanistan, Malaysia, and Singapore including work as domestic servants, construction workers, or garment factory workers face conditions indicative of forced labour.

Special Focus 10

Liberation Tigers of Tamil Eelam (LTTE) - Sri Lanka



The Liberation Tigers of Tamil Eelam ("LTTE") were founded in May 1976 by Vellupillai Prabhakaran with the objective of creating a separate state for Tamils in northern and eastern Sri Lanka.

Ethnic tensions within Sri Lanka, which possesses a majority Sinhalese and a minority Tamil ethnic population, have a long history but emerged most vehemently following the country's independence from British rule in 1948. It was at this point that it became evident that the minority Tamil group (which constitutes the majority population in Sri Lanka's northern and eastern provinces) would be politically marginalized by a system of proportional representation as a result of the greater size of the Sinhalese population nationwide. Such marginalization of the Tamil people, the majority of whom follow the Hindu faith, was emphasized and institutionalized in the 1972 Sri Lanka Constitution, which decreed that the "Republic of Sri Lanka shall give to Buddhism the foremost place" and "it shall be the duty of the State to protect and foster Buddhism".¹⁹

Prabhakaran pursued five principles, which to him justified the LTTE's armed struggle: Recognition of the Tamil as a nation; Recognition of the existence of an identified homeland for the Tamil people; Recognition of the right to self-determination for the Tamil people; Recognition of the right of the Tamil people to separate citizenship; and Recognition of the fundamental right of all Tamils to look on the north and eastern provinces of Sri Lanka as their country. These demands became known as the Thimpu Principles and were presented by the Tamil delegation at the first peace talks of the Sri Lankan Civil War. Prabhakaran also introduced a highly selective recruitment policy favouring Tamils and increased the professionalism of the LTTE's organisation.

Between 1983 and 2009 the conflict between the LTTE and the Sri Lankan government escalated into a civil war. During the period 1983 to 1987 the Indian government, provided arms, training and monetary support to six Sri Lankan Tamil militant groups including the LTTE. During this time the LTTE was just one of several Tamil militant groups operating in Sri Lanka but increasingly established its dominance in the Tamil community as a result of its excellent organisation and

reputation for ruthlessness. In 1987, following direct Indian intervention to broker a peace accord and introduce the Indian Peacekeeping Force (IPKF), the LTTE refused to lay down their weapons and declared war on the IPKF, allegedly ending Indian government funding for the LTTE cause.

The LTTE has since been classified as a terrorist organisation in 32 countries, including India, the US, the UK and the EU and whilst it is now defeated it was at its height regarded for example by the FBI as one of the most dangerous terrorist organisations in the world.

To the present day the LTTE is attributed 12 high level assassinations, including Sri Lankan President Ranasinghe Premadasa and former Indian Prime Minister Rajiv Gandhi, in addition to more than 200 other suicide attacks, and the waging of a 26 year military campaign against the Sri Lankan government that claimed in excess of 70,000 lives. The sophistication of the organisation is aptly demonstrated by its possession of a naval wing known as the Sea Tigers, as well as an air division that in 2007 carried out aerial attacks on Sri Lankan military bases.

In 2009, with the death of leader Velupillai Prabhakaran, the LTTE admitted defeat.²⁰ The group pledged to lay down its arms and the peace has remained unbroken. However, that is not to say that ethnic tensions have evaporated, rather assimilation of Tamils back into Sri Lankan society has been piecemeal and accusations of human rights abuses have been levelled at the Sri Lankan government.

The LTTE financed its operations from a range of sources that included the voluntary and forced contributions of its diaspora community, charities, legitimate businesses and criminal activities. There is some evidence to suggest that LTTE established commercial links with other terrorist organisations. For example, there is evidence which indicates the LTTE provided forged passports to Ramzi Yousef (the man who carried out the first attack against the World Trade Centre in New York in 1993) and that the LTTE stole Norwegian passports and sold them to Al-Qaeda in order to generate funds with which to purchase arms. Some have argued that many of the techniques used by Al-Qaeda have been copied from the LTTE. At its height the LTTE Tamil Tigers was able to raise hundreds of millions of dollars a year, with an estimated 80% of this coming from Tamils in the UK, Canada, Switzerland and Scandinavia. Of the estimated 300,000 Tamils based in the UK, it has been estimated that 20,000 to 30,000 are sympathizers of the LTTE and have been actively engaged in fund raising activities. The Tamil community in the UK is predominantly concentrated in London in places such as Tooting, Mitcham and Harrow. In these communities donating funds to the LTTE has been made easy through the use of the "undiyal" money transfer system. The UK Centre for Social Cohesion has estimated that the LTTE was able to raise £250,000 in donated funds every month from

the UK. There has also been widespread LTTE extortion in the Tamil diaspora based on threats to relatives in Sri Lanka and to prospective donors themselves. Human Rights Watch has presented evidence of LTTE extortion from the Tamil community in Britain based on threats to family members living in Sri Lanka and on more direct personal threats to Tamils living in Britain. It claims that a number of British Tamil associations operate in part as front organisations.

Temples and charities are believed to provide a hub for the co-ordination of financial support for the LTTE. This makes the task of distinguishing donations for legitimate and humanitarian causes from terrorism financing extremely difficult. For example, in 2008 the Sivayogam Trust which ran the Muthuthumaari Amman temple in Tooting (which acts as a focal point for a large population of Tamils who originate from Valvettithurai where Vellupillai Prabhakaran was born and which runs five orphanages in Sri Lanka) had funds frozen by the UK Charities Commission because it suspected that the funds were being sent to the LTTE. In May 2009 the UK's Independent newspaper published an article in which one of the trustees of the charitable wing of the Muthuthumaari Amman temple was quoted as saying "ninety percent of Tamils support the LTTE ideologically but that does not mean they give money to them". When asked whether the temple was still receiving donations for their work abroad, the same trustee reportedly said that "we advise devotees to send [charitable donations] directly instead".

This highlights the fact that there is genuine support for the ideological aims of the LTTE and the ease with which this ideological affinity can be used to legitimise sending funds to the LTTE. It also highlights the risk of donations to the LTTE being pushed out of mainstream channels as a result of official scrutiny and the perceived risk of asset freezing. Funds donated in good faith for humanitarian purposes have historically been susceptible to being diverted for illegitimate ends and the LTTE has sought to capitalise on world events to maximise their revenue generating capabilities. For example, in May 2007, two Tamils with connections to the LTTE were arrested in Australia for raising thousands of dollars under the pretence of being for charities and aid for those affected by the 2004 tsunami which killed 35,000 people in Sri Lanka. In Canada, the World Tamil Movement was designated as a terrorist organisation and the charitable status of the Tamil Refugee Aid Society of Ottawa and the Canadian Foundation for Tamil Refugee Rehabilitation were revoked in 2010 and 2011 respectively.

The LTTE has also engaged in drug smuggling, human trafficking, sea piracy and hijacking, arms smuggling, money laundering, passport forgery and credit card fraud to obtain money to fund the war against the Sri Lankan government. Drug smuggling has been a long standing part of the LTTE's fund raising efforts, netting the organisation US\$200mio a year.

The LTTE had trafficking groups in Thailand, Spain, Switzerland, Italy and France and has been primarily involved in trafficking heroin from Burma and Afghanistan. The Canadian authorities have claimed that the LTTE controls part of the USS1bio drug trade in Montreal and Indian authorities have also claimed LTTE involvement in drug distribution in India. More than 4,000 Tamils have been jailed throughout the world for trafficking narcotics.

World Tamil Movement Canada - Sri Lanka

In 2008, 2 years after it was established in Canada, the World Tamil Movement, which raised funds for the Tamil Tigers from the Canadian tamil community was designated by Canadian authorities as a terrorist organisation. A forensic audit found that WTM was running a pre-authorised payment programme that withdrew monthly sums from the bank accounts of Canadians. The WTM took in up to C\$763,000 a year using the scheme. Whilst some donors participated willingly, others had been coerced or pressurised.

Tamil Rehabilitation Organisation - Sri Lanka

The Tamil Rehabilitation Organisation (TRO) was established in 1985 in Tamil Nadu in south-eastern India by Tamil refugees fleeing the violence in North and East Sri Lanka. Its initial operation was to provide relief to the refugees in India. After the signing of the Indo-Sri Lanka Accord and the subsequent fighting between the LTTE and the Indian Peace Keeping Force, TRO moved its operation and headquarters to Jaffna in Northern Sri Lanka. The headquarters moved again to Killinochchi after Jaffna was taken by Sri Lanka Armed Forces in 1995.

After the signing of the ceasefire agreement in 2002 between the LTTE and the Government of Sri Lanka, TRO was recognised by the Government as a legitimate NGO and was granted NGO status. During the period 2002 to 2005 TRO operated from offices across Sri Lanka in both Government and LTTE controlled areas providing post war and post tsunami relief and rehabilitation to Tamil community. On 15 November 2007, the US Department of the Treasury designated the TRO under Executive Order 13224, aimed to financially isolate US designated foreign terrorist groups and their support network. Under this order, the Department of the Treasury froze all assets held by the TRO and its designees in US territories, and formally prohibited US citizens from transacting with the TRO or its members.

The Department of Treasury stated that "TRO passed off its operations as charitable, when in fact it was raising money for a designated terrorist group responsible for heinous acts of terrorism ... in the US, TRO has raised funds on behalf of the LTTE through a network of individual representatives. According to sources within the organisation, TRO is the preferred conduit of funds from the US to the LTTE in Sri Lanka".

South East Asia



South East Asia is a subregion of Asia, consisting of the countries that are geographically south of China, east of India, west of New Guinea and north of Australia. Southeast Asia consists of two geographic regions: Mainland Southeast Asia, also known as Indochina,

comprising Cambodia, Laos, Burma (Myanmar), Thailand, Vietnam and Peninsular Malaysia, and Maritime Southeast Asia comprising Brunei, East Malaysia, East Timor, Indonesia, Philippines, Christmas Island, and Singapore. The major religions are Islam and Buddhism, followed by Christianity. However, a wide variety of religions are found throughout the region, including many Hindu and animist-influenced practices. The major gangs and groups that operate in the region do so in the so-called Golden Triangle region, and the major terrorist threat is from Islamic terrorist groups that seek the establishment of an Islamic caliphate spanning Indonesia, Malaysia, southern Thailand, Singapore, Brunei, and the southern Philippines.

Indonesia

Indonesia is now the world's third most populous democracy, the world's largest archipelagic state, and the world's largest Muslim-majority nation. The Dutch began to colonize Indonesia in the early 17th century; Japan occupied the islands from 1942 to 1945. Indonesia declared its independence shortly before Japan's surrender, but it required four years of sometimes brutal fighting, intermittent negotiations, and UN mediation before the Netherlands agreed to transfer sovereignty in 1949. Indonesia's first President Soekarno declared martial law in 1957. After an abortive coup in 1965 by alleged communist sympathizers, Soekarno was gradually eased from power. From 1967 until 1988, President Suharto ruled Indonesia with his "New Order" government, becoming authoritarian and seen as fundamentally corrupt such that Transparency International named Suharto in 2004 as being the World's most corrupt leader. After rioting toppled Suharto in 1998, elections took place in 1999, albeit it wasn't until 2004 that the President was elected directly by the people. Susilo Bambang Yudhoyono therefore became Indonesia's first directly elected President and remains President after his re election

In 2005, Indonesia reached a historic peace agreement with armed separatists in Aceh, which led to democratic elections in Aceh in December 2006. Indonesia con-

tinues to face armed resistance in Papua by the separatist Free Papua Movement and from major indigenous terrorist groups, such as Jemaah Islamiyah, who carried out the 2002 Bali Bombings and a loose network of JI spin-off groups, and Jemaah Anshorut Tauhid, which obtain financial support from both domestic and foreign sources.

Most money laundering in Indonesia is connected to non-drug criminal activity such as illegal logging, theft, bank fraud, credit card fraud, maritime piracy, sale of counterfeit goods, gambling and prostitution. Indonesia has a long history of smuggling of illicit goods and bulk cash, facilitated by thousands of miles of unpatrolled coastline, sporadic law enforcement, and poor customs infrastructure. Proceeds from illicit activities are easily moved offshore and repatriated as needed for commercial and personal use.

Corruption remains a serious problem in Indonesia with according to Transparency International, Indonesia ranking 114 out of 175 countries in its 2013 Corruptions Perceptions Index.

In October 2012, the Financial Action Task Force (FATF) placed Indonesia on its Public Statement due to Indonesia's failure make sufficient progress in implementing its AML/CFT action plan. According to the FATF announcement, Indonesia should adequately criminalise terrorist financing; establish and implement adequate procedures to identify and freeze terrorist assets; and amend and implement laws or other instruments to fully implement the International Convention for the Suppression of the Financing of Terrorism.

Jemaah Islamiya - South East Asia/Indonesia

Southeast Asia-based Jemaah Islamiya (JI) is a terrorist group that seeks the establishment of an Islamic caliphate spanning Indonesia, Malaysia, southern Thailand, Singapore, Brunei, and the southern Philippines. More than 300 JI operatives, including operations chief Hamzali, have been captured since 2002, although many are free after serving short sentences. Those released include former JI emir Abu Bakar Bashir who was released from prison in 2006 after serving a 25 month sentence for his involvement in the 2002 Bali Bombings. Indonesia's Supreme Court later that year acquitted him of the charges. Bashir later formed Jamaah Anshorut Tauhid in 2008 and is considered a splinter group at JI with bases across Indonesia. Following the death of top JI bomb maker Azahari bin Husin in November 2005, along with the arrests of several close associates of senior JI operative Noordin Mat Top in 2006, and the 2007 arrests of former acting JI emir Muhammad Naim (a.k.a. Zarkash), JI military commander Abu Dujana, and several of their associates, the operational capabilities of the JI appear to have been reduced, putting an end to the spate of anti-Western attacks that had occurred annually from 2002-2005. The group's most high-profile attack took place in Bali in 2002, when the detonation of three bombs in a tourist district caused the death of 202

people (a total that included 88 Australians, 38 Indonesians, 27 Britons, 9 Americans and 5 Swedes). Analysts have concluded that the attack crippled Bali's tourist-oriented economy and by some estimates reduced Indonesia's overall economic growth by up to 1%. The financial impact of an operation thought to have cost as little as US\$50,000 to plan and execute was therefore considerable. A similar attack was also perpetrated in Bali on 1 October 2005, leaving 26 people dead, including the three suicide bombers. Other major JI attacks include the August 2003 bombing of the J. W. Marriott Hotel in Jakarta, and the September 2004 detonation of a bomb outside Jakarta's Australian Embassy. Prior to these more audacious attacks, in December 2000, JI coordinated bombings of numerous Christian churches in Indonesia and was involved in the bombings of several targets in Manila. In December 2001, Singaporean authorities also uncovered a JI plot to attack the US and Israeli Embassies, and British and Australian diplomatic buildings in Singapore. In February 2004, JI facilitated attacks in Manila, Davao, and General Santos City. Later, in 2007 the group planted an improvised explosive device (IED) in Sultan Kudarat that killed two civilians and injured thirty others. JI associates in the Philippines provide operational support and training for indigenous Muslim militants in the Philippines. The exact organisational strength of JI is currently unknown, however estimates of membership figures vary from the hundreds to one thousand. The group is based in Indonesia and is believed to have cells in Indonesia, Malaysia, and the Philippines. For instance JI associates based in the Philippines provide operational support and training for indigenous Muslim militants. JI is also known to have some links to Al-Qaeda, primarily in the form of funding and training. Despite these links JI has maintained its autonomy, remaining an independent group with its own agenda. Studies of the organisation have revealed that JI has a diverse range of income sources, an approach no doubt designed to make the group more robust in the face of asset seizures and any state crack-down. Revenue reaches the group via individual cash couriers, charities, corporate entities, hawala shops (underground banks), membership contributions, as well as the proceeds from the illegal gold and diamond trade, gun-running, kidnappings, extortion and racketeering.

Jemaah Anshorut Tauhid - Indonesia

Jemah Anshorut Tauhid (JAT) is an Indonesia-based group founded in 2008 by Abu Bakar Bashir, who was also the co-founder and former leader of Jemaah Islamiyah (JI), which was responsible for the 2002 Bali nightclub bombings that killed more than 200 people. JAT seeks to establish an Islamic caliphate in Indonesia, and has carried out numerous attacks on Indonesian Government personnel and civilians in order to achieve this goal. Abu Bakar Bashir, the founder and leader of JAT, was convicted and sentenced to prison in 2011 for his role in organizing a militant training camp in Aceh. JAT has robbed banks and carried out other illicit activities to fund the purchase of assault weapons, pistols, and

bomb-making materials. On 25 September 2011, a JAT suicide bomber detonated explosives inside a church in Central Java, killing the bomber and wounding dozens. Indonesian police arrested other JAT members in connection with this bombing and uncovered a plot for additional suicide attacks. In April 2011, a suicide bomber carried out an attack at a mosque in West Java that injured dozens of police officers and killed the bomber.

Free Papua Movement - Papua New Guinea

The former Dutch colony of West Papua, the western half of the island of New Guinea, came under temporary Indonesian control as part of a UN-managed "decolonisation" of the Dutch East Indies in 1963. It became a permanent part of Indonesia in 1969. The Free Papua Movement (OPM) is a political organisation that seeks independence from Indonesia for the indigenous people of West Papua. Insurgent operations against the Indonesian government and security forces are run by the group's military wing, the Liberation Army of the Free Papua Movement. The OPM's fundamental goal is self-rule combined with a return to a traditional mode of life. The group conducts small-scale raids and attacks on government offices and military installations, including a weapons depot in 2003. Members of OPM often retreat into Papua New Guinea to hide. Material support has been provided by both Libya and the New People's Army.

Malaysia

During the late 18th and 19th centuries, Great Britain established colonies and protectorates in the area of current Malaysia. These were occupied by Japan from 1942 to 1945. In 1948, the British-ruled territories on the Malay Peninsula except Singapore formed the Federation of Malaya, which became independent in 1957. Malaysia was formed in 1963 when the former British colonies of Singapore, as well as Sabah and Sarawak on the northern coast of Borneo, joined the Federation. The first several years of the country's independence were marred by a communist insurgency, Indonesian confrontation with Malaysia, Philippine claims to Sabah, and Singapore's withdrawal in 1965. During the 22-year term of Prime Minister Mahathir bin Mohamad (1981-2003), Malaysia was successful in diversifying its economy from dependence on exports of raw materials to the development of manufacturing, services, and tourism. Prime Minister Mohamed Najib bin Abdul Razak (in office since April 2009) has continued these pro-business policies and has introduced some civil reforms. Malaysia has established an offshore financial center on the island of Labuan which is home to both domestic and foreign banks and insurers.

Malaysia's long porous land and sea borders and its strategic geographic position increase its vulnerability to transnational criminal activity, including money laundering and terrorist financing. Malaysia is primar-

ily used as a transit country to transfer drugs originating from the southeastern Asian Golden Triangle and Europe. Drug trafficking is an important source of illegal proceeds in Malaysia. Iranian and Nigerian drug trafficking organisations are the main sources of illegal proceeds. Corruption is also considered a significant money laundering risk. Other crimes generating significant criminal proceeds in Malaysia include fraud, illegal gambling, credit card fraud, counterfeiting, robbery, forgery, human trafficking, extortion and smuggling. Smuggling of goods subject to high tariffs is a major source of illicit funds. Malaysia is a destination and, to a lesser extent, a source and transit country for women and children subjected to conditions of forced labour and women and children subjected to sex trafficking.

A number of terrorist organisations have been active on Malaysian territory, including *Jemaah Islamiyah* and *Abu Sayyaf*, whose aims include the establishment of an Islamic State encompassing Malaysia but also Borneo and the Philippines and south Thailand. Terrorist financing in Malaysia is predominantly carried out using cash and relies on trusted, clandestine networks.

Philippines

The Philippine Islands became a Spanish colony during the 16th century, which were ceded to the US in 1898 following the Spanish-American War. In 1935 the Philippines became a self-governing commonwealth. In 1942 the islands fell under Japanese occupation during World War II, and US forces and Filipinos fought together during 1944-45 to regain control. In 1946 the Republic of the Philippines attained its independence. A 20-year rule by Ferdinand Marcos ended in 1986, when a "people power" movement in Manila forced him into exile and installed Corazon Aquino as president. Her presidency was hampered by several coup attempts that prevented a return to full political stability and economic development. Fidel Ramos was elected president in 1992. His administration was marked by increased stability and by progress on economic reforms. In 1992, the US closed its last military bases on the islands. Joseph Estrada was elected president in 1998. He was succeeded by his vice-president, Gloria Macapagal-Arroyo in 2001 after Estrada's impeachment trial on corruption charges broke down and another "people power" movement demanded his resignation. Macapagal-Arroyo was elected for a six-year term as president in May 2004, with her term also marred by several corruption allegations. Current President Benigno Aquino III was elected for a six-year term as president in May 2010. The Philippine Government faces threats from several terrorist groups. Manila has waged a decades-long struggle against ethnic Moro insurrections in the southern Philippines, which has led to a peace accord with the Moro National Liberation Front and ongoing peace talks with the *Moro Islamic Liberation Front*. The decades-long Maoist-inspired New People's Army insurgency also op-

erates through much of the country. The Abu Sayyaf, a radical Islamic terrorist group, is active in the Southern Philippines and Malaysia, looking to establish an Islamic State in the region. It was responsible for the *Superferry 14* bombing in 2004. Also active with similar goals is *Jemaah Islamiyah*, whose members were responsible for the *Bali Bombings* in 2002.

Corruption remains a serious problem in the Philippines and a source of laundered funds. Smuggling, particularly bulk cash smuggling, is also a major problem. The Philippines continues to experience foreign organised criminal activity from groups in China, Hong Kong and Taiwan. In addition, insurgent groups operating in the Philippines engage in money laundering through ties to organised crime and criminal activities are partially funded through kidnapping for ransom as well as drugs and arms trafficking. The Philippines has a domestic methamphetamine problem which is growing. Marijuana is produced mainly in rural areas where Manila's control is limited but mainly for domestic use. Remittances sent to the Philippines by its large expatriate community also provide a channel for money laundering, however the bulk of these are captured by banks and money remitters.

Abu Sayyaf (ASG) - Philippines/Malaysia

The Abu Sayyaf Group (ASG), whose name translates to mean "Father of the Sword" in Arabic, is a radical Islamic terrorist group active in the Southern Philippines and Malaysia. Its stated goal is the creation of an independent Islamic state encompassing the areas of Southern Thailand, the island of Borneo, the Sulu Archipelago, and Mindanao, all of which are dominated by the Moro Muslim ethnic group. In order to fully comprehend the social milieu from which Abu Sayyaf emerged in the 1990s it is necessary to retrace the history of the Philippines back to the days of Spanish colonization. During this period, the nation experienced what has been described as 'evangelization with the sword' as Spanish colonizers attempted to replace all native denominations with the Christian faith. This proved a largely successful process, however one Muslim tribe in the country's south known as the Tausug remained unconquered. Following the Second World War this southern part of the Philippines suffered further Christian incursions when the government relocated many Christians from the north to the area. Land grabbing and much social strife ensued, finally expressing itself in the Moro Wars of the 1970s. It was from this environment of deep-seated ethnic and religious conflict that Abu Sayyaf surfaced in 1991. The ASG was founded by Abdurazzak Janjalani and other like-minded members of the Moro National Liberation Front (MNLF) who were dissatisfied with its leadership. In particular the MNLF's negotiations with the Philippine government were deemed unacceptable by these more radical militants. The ASG's principal founder, Abdurazzak Janjalani, was a Muslim cleric previously recruited and trained by bin Laden's *Al-Qaeda* in Afghanistan. Links between the two terrorist groups are believed to have been maintained, with

several of the AQ members responsible for executing the attacks on the US World Trade Centre in 2001 known to have undertaken numerous visits to the Philippines. The ASG also aligned itself with AQ's jihad against "Zionists and Crusaders" in 1998. Today Abu Sayyaf is renowned for seizing international hostages and possesses a gruesome reputation for beheading its victims. However the group was brought most forcefully into the consciousness of the international community by its links to an audacious three-phase terrorist attack during the mid-1990s. Known as the *Bojinka Plot*, the attack was to begin with the assassination of Pope John Paul II, followed by the bombing of 11 passenger planes bound for the US, and finally the hijacking and crashing of a plane into the CIA's headquarters in Virginia. While the plot was ultimately abortive, its scope revealed the ASG to be a highly dangerous terrorist organisation committed to causing large scale civilian losses. This commitment was again demonstrated in 2004 by the bombing of *Superferry 14* as it set sail from Manila; an attack that resulted in 116 fatalities. The organisation's funding, at least at its outset, is believed to have been supplied by bin Laden's brother-in-law Muhammad Jamal Khalifa. Khalifa has generated considerable amounts of money to finance terrorist operations via various charities such as the International Islamic Relief Organisation via its Philippine branch. In a leaked report by Colonel Rodolfo Mendoza of the Philippines it emerged that Khalifa had founded at least 8 front organisations in order to channel revenue to terrorist groups, including Abu Sayyaf. The ransoming of hostages, along with the extortion of Filipino communities is also known to provide part of the group's income. In terms of membership figures, the ASG was in 2003 believed to number less than 500 core militants, though its support network could number in the thousands. In 2002 the threat posed by the ASG was deemed sufficient to warrant the deployment of 600 US troops in the Philippines as part of the post 9/11 War on Terror. The military campaign was, however, a failure and a year later US troops withdrew having failed to eradicate the group. Today the ASG continues military operations in the Philippines, clashing in February 2013 with its former parent organisation the Moro National Liberation Front. The dispute arises following the MNLF's signing of a peace agreement with the Philippine government. Despite the agreement offering the Moro Islamic community broad autonomy, the ASG is one of several groups that have refused to adhere to a settlement.

New People's Army (NPA) - Philippines

The New People's Army was founded in 1969 in the Philippines as the armed wing of the outlawed Communist Party of the Philippines, Marxist-Leninist (CPP-ML). The group was formulated by 11 left-wing Filipino radicals who established as their goal the realisation of a socialist state. This socialist transformation of the Philippines was to be brought about by armed revolution, and as outlined by Maoist theory, would rely on the guerrilla warfare of a peasant population in revolt. On its inception the NPA constituted a small group

based in the mountainous areas of central and northern Luzon. In its early months any measure of military prowess at the group's disposal was provided by a group of agrarian rebels, and the NPA's meagre armoury is believed to have been made up of 70 weapons at most. Operating from a headquarters in northern Luzon the group attempted to use the area's natural caves as means of evading government forces. However within just a few weeks of the NPA's first operations it was forced to retreat into ever more remote hideouts in northern Luzon. Between 1969 and 1976 the NPA received considerable material support from the People's Republic of China, however when this aid ceased in 1976 the group entered a troubled five years in which its strength declined considerably. Nevertheless, having found alternative revenue sources such as the extortion of foreign businesses and the levying of taxes from supporters, the group had recovered by the early 1980s and experienced considerable growth in the following years. For instance by 1986 and the removal of *President Ferdinand Marcos* from power, the NPA had established a footing in 62 of the country's 73 provinces and commanded as many as 26,000 armed militants. The organisation's main support bases were located in the Filipino countryside and amongst the rural population though the NPA did receive notable support in Davao City. Despite the considerable size of the NPA its military capacities were far outweighed by those of the Filipino government. Consequently the NPA focussed on ambushes, assassinations and swift raids. High priority NPA targets have been Filipino politicians, security officials and news reporters. In terms of military control, the NPA could hold little ground by following the traditional guerrilla tactic of dispersing into forests and mountains after engagements, however in many rural areas the NPA and its parent CPP-ML organisation established itself as the de-facto government during the mid-1980s. Not only would the group levy taxes, but in many cases directed social services such as health care and sanitation. In 2002 the NPA was designated a terrorist organisation by the US, with the EU reaching the same conclusion in 2005. NPA attacks continued into 2011. However since the organisation's delisting as a terrorist group by the Government of the Philippines in 2011 peace talks began. Whilst hopes were raised that peace could be achieved after 44 years of insurgency and before President Benigno Aquino's term ends in 2016, peace talks collapsed in May 2013, and the NPA returned to former ways, attacking a major mining company in Central Philippines killing 5 soldiers and burning equipment and buildings. Today the NPA is believed to number around 10,000 members.

The Moro Islamic Liberation Front - Philippines

The Moro National Liberation Front (MNLF) was an Islamist group formed in the 1960s in the Southern Philippines. The group was most active in the Bangsamoro region of Mindanao, the Sulu Archipelago, Palawan, Basilan and other neighboring islands, operating with the aim to establish an independent Muslim nation. Whilst an offer of semi-autonomy in 1976 was accepted

by some it was also rejected by others, leading to the formation of a breakaway group, the Moro Islamic Liberation Front (MILF) who rejected government offers until 2007, when the Philippine government offered to recognise the right of self-determination for the Moro people which it had never done in three decades of conflict. Still it took until 2012, until President Benigno Aquino announced a firm peace deal with the MILF stating that "This framework agreement paves the way for a final and enduring peace in Mindanao". MILF Vice Chairman Ghazali Jaafar is quoted as saying "We are very happy. We thank the president for this." The deal was signed on 15 October 2012. Its aim is to pave the way to enduring peace between the two parties by officially envisaging an autonomous region in Mindanao. According to the peace deal, this semi-independent Muslim area would have a more just share of revenues from the extraction of resources, budgetary autonomy, its own police, and sharia law only for Muslims and in exchange the MILF will stop armed resistance against the government for autonomy and will allow the national government to retain its control of national security and foreign policy. The autonomy agreement to be gradually implemented will also rename the region Bangsamoro after the Moro people.

Rajah Solaiman Movement - Philippines

The Rajah Solaiman Movement (RSM) is a small terrorist organisation dedicated to creating an Islamic state in the Philippines. Founded in 2002, the group is named after Rajah Solaiman, a Muslim, who was the last indigenous King of Manila before Spanish rule began in the 1500s. RSM maintains close relationships with other terrorist groups including the ASG, Jemaah Islamiyah (JI), and the Moro Islamic Liberation Front (MILF). RSM is known to share members, training facilities, and funds with these terrorist organisations. One Filipino Army official speculated that generally, ASG plans operations, JI supplies funding, MILF provides safe houses for operatives, and RSM executes operations. Using illegitimate Filipino Islamic charities and its relationships with other prominent regional terrorist groups, RSM is able to fund its activities. Increasingly, it receives funding from sources in Saudi Arabia and other countries in the Middle East. RSM is suspected of acting in concert with the ASG, for example it was also involved in the Valentine's Day Superferry bombing that killed over 116 people in 2004.

Vietnam

Vietnam became independent from Imperial China in 938 AD, and successive royal dynasties flourished as the nation expanded into Southeast Asia until the Indochina Peninsula was colonized by the French in the mid-19th century. The name Vietnam translates as "Southern Viet". France took full control of Vietnam in 1884, becoming part of French Indochina in 1887, joining with Cambodia and later adding Laos. Following a Japanese occupation in the 1940s, the Vietnamese

fought French rule in the First Indochina War, with communist forces under Ho Chi Minh eventually expelling the French in 1954. In a peace deal, Vietnam was divided into the communist North and anti-communist South. US economic and military aid to South Vietnam grew through the 1960s in an attempt to bolster the government, and escalated into a full scale war, with US forces defeated and withdrawn in 1973. The country was reunited in 1975 and a one-party system led by the Communist Party of Vietnam (CPV), has ruled since unification. Since 2000, Vietnam's economic growth rate has been among the highest in the world, following successful economic reforms. The most recent presidential elections held 2011, saw Truong Tan Sang, the incumbent, re-elected by the deputies (members) of the National Assembly. Vietnam has an estimated 90.3 million inhabitants as of 2012 and it is the world's 13th-most populous country, and the eighth-most populous Asian country. Vietnam's economy is largely cash-based, with both US\$ and gold widely used as a means of exchange and storing value. Sources of illicit funds in Vietnam include public corruption, fraud, gambling, prostitution, counterfeiting of goods and trading in counterfeit merchandise, illegal wildlife trade, and trafficking in persons. Remittances from the proceeds of narcotics trafficking in Canada, the UK, and the US are a significant source of money laundering, as are narcotics proceeds from traffickers using Vietnam as a transit country. Vietnam's banking sector is considered at risk due to a large government ownership and control and at risk for money laundering. Corruption remains a serious problem in Vietnam with according to Transparency International, Vietnam ranking 123 out of 174 countries in its 2012 Corruption Perceptions Index. The Financial Action Task Force (FATF) included Vietnam in its Public Statement, acknowledging that, although Vietnam has taken steps toward improving its anti-money laundering/counter-terrorist financing (AML/CFT) regime, Vietnam has not made sufficient progress in implementing its action plan, and certain strategic AML/CFT deficiencies remain.

Golden Triangle Cartels

The Golden Triangle, stretching across Myanmar, Thailand and Laos, has been one of the world's leading production centres of heroin for decades. Myanmar is the most predominated origin state in the region. More than three quarters of Myanmar's production supplies the local and regional markets, mainly Chinese market. The rest flows to other Southeast Asian countries. Criminal gangs and insurgent groups are involved in trafficking drugs, humans, wildlife, gems, timber, and other contraband. Widespread collusion between organised gangs, traffickers and Myanmar's ruling military junta, is suspected. In addition most of the insurgent groups are also organised crime groups. There were at least 16 different armed groups controlling parts of the Shan State and the Kayah State. Being isolated from other sources of income, many of the insurgent groups

turned to taxing of drug production as a major source of revenue as well as taxing timber, gems, and other black-market goods passing through the territories which they control. One major business interest for organised criminal gangs include illegal gambling, particularly in the border area and operating in some hotels.

Thailand

A unified Thai kingdom, known as Siam was established in the mid-14th century, changing its name in Thailand in 1939. Thailand is the only Southeast Asian country never to have been taken over by a European power. A bloodless revolution in 1932 led to a constitutional monarchy. In alliance with Japan during World War II, Thailand became a US ally in 1954 after sending troops to Korea and later fighting alongside the US in Vietnam. Since 2005, Thailand has experienced political turmoil including a military coup in 2006 that ousted then Prime Minister Thaksin Chinnawatra (criticisms and allegations of corruption) and then followed by large-scale street protests by competing political factions ever since. In 2011, Thaksin's youngest sister, Yingluck Chinnawatra, won elections and assumed control of the government, but the government is struggling to survive with opposition demonstrations demanding a change in the government. Thailand has an extremely porous border and is vulnerable to money laundering within its own underground economy as well as to many categories of cross-border crime, including contraband smuggling including illicit narcotics where Thailand is a minor producer of opium, heroin, and marijuana and a transit point for illicit heroin en route to the international drug market from Myanmar and Laos. Thailand is a source, transit, and destination country for international migrant smuggling and trafficking in persons, a production and distribution center for counterfeit consumer goods and a center for the production and sale of fraudulent travel documents. The proceeds of illegal gaming, corruption, underground lotteries, and prostitution are laundered through the country's financial system. The Thai black market includes a wide range of pirated and smuggled goods, from counterfeit medicines to luxury automobiles. Money launderers and traffickers use banks, as well as non-bank financial institutions and businesses, to move the profits of narcotics trafficking and other criminal enterprises. In the informal money changing sector, there is an increasing presence of hawalas via money shops that service Middle Eastern travellers in Thailand. Thailand was publicly identified by the Financial Action Task Force (FATF) in February 2010 for its strategic anti-money laundering/counter-terrorist financing (AML/CFT) deficiencies, for which it has developed an action plan. In October 2012, the FATF determined that Thailand's progress against the agreed action plan's timeline continues to be insufficient and the Government of Thailand (GOT) needs to take adequate action to address its main deficiencies. Since January 2004, thousands have been killed and wounded in violence associated with the ethno-nationalist insur-

gency in Thailand's southern Malay-Muslim majority provinces which prompt border closures and controls with Malaysia to stem insurgent activities.

Jao/Chao Pho - Thailand

Primarily ethnic Chinese in Thailand using legitimate businesses as fronts for crime and infiltration of the police, military and government. As a result of its name, which translates literally as 'godfather', this group has often been considered simply as Thailand's expression of the Italian-American style gangster that its name evokes. This is however a misconception. The Chao Pho demonstrate many characteristics of traditional Thai leaders known as the nak leng. These leaders were considered firm but generally fair, and showed particular loyalty to their fortunate benefactors. As a result Nak Leng and the Chao Pho that have come to replace them in many of Thailand's provinces, maintain their seats of power by a mixture of intimidation, bribery and indeed support. Today Chao Pho, despite their links to criminal enterprise, maintain close connections with high ranking state officials. Common criminal activities amongst Chao Pho include corruption, illegal gambling such as the underground lottery, prostitution and drug trafficking. They have also traditionally had dealings with more mainstream financial institutions, forging particularly close knit connections with Thailand's rural banks. As late as the 1960s Chao Pho played an important role in provincial bank branches, ensuring that repayments were made and attracting new clients. Banks have also been used as depositories for the illegal funds generated through schemes such as the underground lottery. The Chao Pho did not however conduct only illegal business; rather they expanded into legitimate commerce, most notably construction, logging, transportation and the distribution of whiskey. Politics also became a major occupation of the Chao Pho from the 1970s onwards, at first using their networks of influence to support chosen figures, but later standing in elections themselves.

Laos

Modern-day Laos has its roots in the ancient Lao kingdom of Lan Xang, established in the 14th century. For 300 years Lan Xang had influence reaching out from Laos into present-day Cambodia and Thailand. Laos was then dominated first by Siam (Thailand) and then from the late 18th century as part of French Indochina. In 1975, Communists took control of the government ending a six-century-old monarchy and instituting a strict socialist regime closely aligned to Vietnam, which has since liberalized, particularly as regards private enterprise. Along with China, Cuba, Vietnam, and North Korea, Laos is one of the world's five remaining socialist states, whose government is headed by President Choummaly Sayasone and Prime Minister Thongsing Thammavong. Laos is positioned at the crossroads of mainland Southeast Asia's drug trade, with also an estimated domestic opium poppy cultivation problem too and with corruption endemic, bulk cash smuggling

commonplace, it's easy to see why Laos is vulnerable to money laundering activities. Furthermore, the gaming industry, primarily driven by Chinese tourists visiting casinos in Special Economic Zones near the border, continue to present money laundering opportunities outside of the formal financial sector.

Myanmar

Myanmar (also known as Burma) is the second largest country in Southeast Asia, with a population of over 60 million. Myanmar is subject to certain Sanctions and Embargoes, for details see Part 1, Section 3, Money Laundering Laws and Regulations: Sanctions and Embargoes above. Myanmar is predominately a cash-based economy with less than 20% of the population accessing the formal banking system. It is also a "US dollarised" economy with US dollars readily accepted at shops and retail outlets. Myanmar was once one of the wealthiest countries in Southeast Asia. However, in 1962 General Ne Win overthrew the elected civilian government and replaced it with a repressive military government, regularly accused of Human rights abuses. The military government isolated Myanmar from the international community and poor economic performance followed. The military government was criticised by most of the international community for using force to respond to demonstrations in 1988 and refusing to honor the results of the 1990 elections in which the National League for Democracy (NLD) led by Aung San Suu Kyi received 62% of the votes cast, taking some 80% of the 485 seats contested. In response to the human and political rights issues in Myanmar, the US imposed economic sanctions against the country in 1990, which were followed by Sanctions from others, including the EU. Improvements under leader Thein Sein who took over from former dictator, General Than Shwe in 2010 led to reform negotiations with Aung San Suu Kyi and it appears Myanmar is now set on a new course after decades of military rule. The political reforms included allowing Aung San Suu Kyi to run for parliament and releasing political prisoners. In response, EU and Switzerland as well as the US suspended most of the sanctions against Myanmar. Myanmar remains one of the most corrupt countries in the world. In the most recent Corruption Perception Index in 2013 published by Transparency International, Burma's rank was 157 out of 175. The only countries that ranked worse were Somalia and North Korea. For decades, Burma's military leaders divided up the country's national wealth among themselves and their business friends, for example most recently in 2010-11, by transferring state assets, especially real estate, to military families under the guise of a privatization policy further widening the gap between the economic elite and the public, many of whom live in poverty. Terrorism in Myanmar primarily consists of anti-government militant activity. Militant separatists in India, such as the United Liberation Front of Assam and the United National Liberation Front, have bases in Myanmar from which they launch attacks into India.

Notable incidents in Myanmar include the 1983 Rangoon bombing, allegedly by North Korean agents, and three bombings on 7 May 2005 in the capital which killed 11 and injured more than 150. Ethnic rebels were blamed. Transnational or major organised crime groups, for example Jao/Chao Pho, United Wa State Army/Red Wa and Khun Sa Cartel operate in Myanmar and in particular in the Golden Triangle region.

Khun Sa Cartel - Myanmar

"Money Tree" to his supporters and "Prince of Death" to his foes, Khun Sa was a drug trafficker and self-proclaimed freedom fighter operating in Myanmar. Khun Sa was a guerrilla fighter originally fighting for the independence and creation of a "Shan" state from Burma before turning to the drugs trade in the 1960s. Having left the Myanmar army Sa set about establishing his own private army and embarked on conflicts with other drug trafficking groups. The fighting was dubbed the Opium Wars and proved highly unsuccessful, leaving his organisation in tatters and Sa himself behind bars. However after his release in 1974 and the arrest of the area's other foremost drug lord, Sa flourished and as a result Sa's power grew to such an extent that it is estimated that 20,000 men served amongst the ranks of his private army at the height of its strength, and Sa's network is believed to have controlled around half of all the opium produced in the Golden Triangle annually. Khun Sa also boasted a vast legal commercial empire. In 1999 Sa was arrested by Myanmar troops, however the country refused to allow his extradition to the US for trial on drug trafficking charges despite a US\$2mio reward being offered by the US. Instead Khun Sa was allowed by Burma's ruling generals to live out the rest of his life in Rangoon until his death in 2007.

United Wa State Army or Red Wa - Myanmar

The United Wa State Army, also known as Red Wa, is based in Myanmar's Special Region Number 2 and is the military wing of the United Wa State Party. Founded by Chao Ngi Lai and later led by Bao Youxiang, the organisation emerged after the collapse of the Communist Party in Burma and received strong support from China. The group has emerged as one of Southeast Asia's foremost drug producers, manufacturing methamphetamine and heroin with very little intervention from the Myanmar government. This immunity from prosecution was further strengthened by a 2008 constitutional ruling that awarded the United Wa State Army control of two "self administered" districts in northeastern Shan state. Consequently Myanmar has emerged as the second highest opium producing state in the world, surpassed in 2011 only by Afghanistan. This large scale involvement in the drugs trade serves primarily to fund the UWSA's resistance to the Myanmar government; financing the group's 30,000 strong standing army. Alongside the production and trafficking of opium, the UWSA also levies illegal taxes that are little different from outright extortion.

Eastern Asia



More than 1.5 billion people, about 38% of the population of Asia or 22% of all the people in the world, live in East Asia, including China & Taiwan, Japan, N & S Korea, and Mongolia. Historically, many societies in East Asia have been part of the Chinese cultural sphere, and East

Asian vocabulary and scripts are often derived from Classical Chinese and Chinese script. The history of East Asia is predominantly the Chinese Dynasties but also the great empires built at home and conquered abroad. East Asians made an impact outside of their region, including not only into Central Asia but also into the heart of Europe. For example both Attila the Hun and Genghis Khan were two of the greatest conquerors the world has ever known. Attila the Hun, in the early 5th Century AD ruled over an empire that stretched from modern-day Uzbekistan to Germany, and from the Baltic Sea in the north to the Black Sea in the south. His people, the Huns, moved west to Central Asia and Eastern Europe after leaving the East Asian homelands. Genghis Khan, a Mongol leader in the late 12th Century conquered an empire larger than Rome's at the peak of its power. Still East Asia is best known for its Chinese Rulers who dominated in trade as well as military, such as the Qin and the Han Dynasties. There are records of tributes sent overseas from the early kingdoms of Korea and Japan, but as connections began to strengthen with the Western world, Chinese power began to diminish. Japan took the opportunity to begin conquering colonies. At the time of the start of WWII, Korea, Taiwan and the Northeastern part of China were all under Japanese control. It was not until the end of WWII when Korea and Taiwan had a chance to free themselves from Japan.

According to the UN Office on Drugs and Crime (UNODC), in its report "Transnational Organised Crime in East Asia and the Pacific: A Threat Assessment" organised crime groups dealing in fake goods, drugs, human trafficking and illicit wildlife trade earn nearly \$90 billion annually in East Asia and the Pacific. It estimates that the trade in counterfeit goods earns most (US\$24.4bio), followed by illegal wood products (US\$17bio), heroin (US\$16.3bio) and methamphetamines (US\$15bio). Fake medicines (US\$5bio), the black market trade in used electronics components to avoid legitimate recycling (US\$3.75bio) and the illegal wildlife trade (US\$2.5bio). Migrant smuggling and the trafficking of women and girls for prostitution or general labour also earn hundreds of millions of dollars each year.

China



According to Chinese tradition, the first imperial dynasty was the Xia, who emerged around 2000 BC. The first Chinese dynasty that left historical records, the loosely feudal Shang, settled along the Yellow River in eastern China from the 17th to the 11th century BC. The Shang

were conquered by the Zhou, who ruled between the 12th and 5th centuries BC who centralized authority was slowly eroded by feudal warlords. Many independent states eventually emerged from the weakened Zhou state, and continually waged war over 300 years. By the time of the 5th–3rd centuries BC there were seven powerful sovereign states in what is now China, each with its own king, ministry and army. The Warring States period ended in 221 BC after the state of Qin conquered the other six kingdoms and established the first unified Chinese state. The word "China" is commonly thought that the word is derived from the Qin Dynasty.

The Great Wall of China was built by several dynasties over two thousand years to protect the sedentary agricultural regions of the Chinese interior from incursions by nomadic pastoralists of the northern steppes. The subsequent Han Dynasty ruled China between 206 BC and 220 BC and created a lasting Han cultural identity among its populace that has endured to the present day. The Han Dynasty expanded the empire's territory considerably with military campaigns reaching Korea, Vietnam, Mongolia and Central Asia, and also helped establish the Silk Road in Central Asia. Han China gradually became the largest economy of the ancient world. The Han Dynasty adopted Confucianism, a philosophy developed as its official state ideology.

In the 13th century, China was gradually conquered by the Mongol empire. In 1271, the Mongol leader Kublai Khan established the Yuan Dynasty, which itself was overthrown in 1368 with the establishment of the Ming Dynasty. Under the Ming Dynasty, China enjoyed another golden age, developing one of the strongest navies in the world and a rich and prosperous economy amid a flourishing of art and culture. It was in this period that China's capital was moved from Nanjing to Beijing. The Qing Dynasty, which lasted from 1644 until 1912, was the last imperial dynasty of China.

In the 19th century, the Qing Dynasty experienced Western imperialism following two Opium Wars with Britain. China was forced to sign unequal treaties, pay compensation, allow extraterritoriality for foreign nationals, and cede Hong Kong to the British. The First

Sino-Japanese War (1894–95) resulted in Qing China's loss of influence in the Korean Peninsula, as well as the cession of Taiwan to Japan. The weakening of the Qing regime led to increasing domestic disorder and numerous rebellions as well as famine. In the 19th century, the great Chinese Diaspora began. The ill-fated anti-Western Boxer Rebellion of 1899–1901 further weakened the Qing Dynasty. The Xinhai Revolution of 1911–12 brought an end to the Qing Dynasty and established the Republic of China (1912–1949) which was established and led by Sun Yat-sen of the Kuomintang (the KMT or Nationalist Party) and later under Chiang Kai-shek. In 1927 the Chinese Civil War was fought between the Kuomintang and the Communists until Japanese aggression and the Second Sino-Japanese War (1937–1945), a part of World War II, forced an uneasy alliance between the Kuomintang and the Communists. Japanese forces committed numerous war atrocities against the civilian population; in all, as many as 20 million Chinese civilians died. An estimated 200,000 Chinese were massacred in the city of Nanjing alone during the Japanese occupation. Japan unconditionally surrendered to China in 1945.

Major combat in the Chinese Civil War ended in 1949 with the Communist Party Chairman Mao Zedong proclaimed the establishment of the People's Republic of China in control of mainland China, and the Kuomintang retreating to Taiwan.

Mao encouraged population growth, and under his leadership the Chinese population almost doubled from around 550 million to over 900 million. However, Mao's Great Leap Forward, a large-scale economic and social reform project, resulted in an estimated 45 million deaths between 1958 and 1961, mostly from starvation. Between 1 and 2 million landlords were executed as "counterrevolutionaries." In 1966, Mao and his allies launched the Cultural Revolution, sparking a period of political retribution and social upheaval which lasted until Mao's death in 1976. In October 1971, the PRC replaced the Republic of China in the UN, and took its seat as a permanent member of the Security Council. After Mao's death in 1976 and the arrest of the faction known as the Gang of Four, who were blamed for the excesses of the Cultural Revolution, Deng Xiaoping took power and led the country to significant economic reforms. The Communist Party subsequently loosened governmental control over citizens' personal lives and the communes were disbanded in favor of private land leases. This turn of events marked China's transition from a planned economy to a mixed economy with an increasingly open market environment. Deng developed "Socialism with Chinese characteristics" and Chinese economic reform, also known as the "socialist market economy", and opened China to the global market. Deng is famous for saying in a 1977 speech that; "It doesn't matter whether the cat is black or white, as long as it catches mice." He also compared Chinese Politics to American remarking that; "the US brags about its political system, but the [American] President says one

thing during the election; something else when he takes office, something else at midterm and something else when he leaves." China adopted its current constitution on 4 December 1982. In 1989, the violent suppression of student protests in Tiananmen Square brought worldwide condemnation and sanctions against the Chinese government.

President Jiang Zemin and Premier Zhu Rongji led the nation in the 1990s. Under their administration, China's economic performance pulled an estimated 150 million peasants out of poverty and sustained an average annual gross domestic product growth rate of 11.2%. The country formally joined the World Trade Organisation in 2001, and maintained its high rate of economic growth under Hu Jintao's presidency in the 2000s. However, rapid growth also severely impacted the country's resources and environment, and caused major social displacement. Living standards continued to improve rapidly despite the late-2000 recession, but centralized political control remained tight. Preparations for a new Communist Party leadership change in 2012 were marked by factional disputes and political scandals. During China's 18th National Communist Party Congress in November 2012, Hu Jintao and Wen Jiabao were replaced as President and Premier by Xi Jinping and Li Keqiang, who formally took office in 2013.

China Designated Terrorist Organisations

China Ministry of Public Security issued a list in 2003 of terrorist organisations, focussed on East Turkistan, listing the following organisations:²¹ the Eastern Turkistan Islamic Movement (ETIM); the Eastern Turkistan Liberation Organisation (ETLO); the World Uyghur Youth Congress (WUYC) and the Eastern Turkistan Information Center (ETIC).

The Chinese government alleges that ETIM is comprised of eight major factions, which are committed to terrorist attacks in the name of an Eastern Turkistan Islamic state: Central Asian Uygur Hezbollah (Kazakhstan), East Turkistan Liberation Organisation (ETLO), Eastern Turkistan International Committee, Eastern Turkistan Islamic Movement (Afghanistan), Eastern Turkistan Islamic Resistance Movement (Turkey), Eastern Turkistan Youth League (Switzerland), Turkistan Party (Pakistan), and the United Committee of Uyghurs' Organisations (Central Asia).

It is unclear whether or not most of these are actual terrorist groups, and if so whether or not these are actual factions of ETIM. ETLO's known to be a terrorist group that supports ETIM's cause and could possibly be an ally of ETIM as well. ETIM has been implicated in terrorist plots against US interests in the Central Asia region, including a foiled plot to attack the US Embassy in Kyrgyzstan.

World Uyghur Youth Congress - China/Xinjiang

Xinjiang is the north western province of China, about twice the size of Turkey and home to about 9 million

Uyghurs, many of whom complain about religious and cultural suppression by Chinese authorities and seek the establishment of a self-governing, independent state called East Turkistan. Some of the more important groups that support independence for East Turkistan and also labelled terrorist organisations, by Chinese and/or the US include the World Uyghur Youth Congress, East Turkistan Information Centre, East Turkistan Islamic Movement and East Turkistan Liberation Organisation.

The Eastern Turkistan Islamic Movement - China/Xinjiang

The Eastern Turkistan Islamic Movement (ETIM) is an Islamist extremist group based in China's Xinjiang-Uyghur Autonomous Region. ETIM is an ethnic Uyghur separatist organisation that aims to create an Islamist state in the Xinjiang province. The area commonly referred to as Turkistan is sometimes split into Western Turkistan and Eastern Turkistan.

Western Turkistan was controlled by the Russian empire and then by the USSR, and so the area is also referred to as Russian Turkistan.

The USSR treated this area as an autonomous region. Following the dissolution of the USSR, the region was split among five new republics, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan.

In contrast, Eastern Turkistan has long been a part of China and is sometimes referred to as Chinese Turkistan. Today, the region is officially referred to as the Xinjiang-Uyghur Autonomous Region. While the Eastern Turkistan Islamic Movement's name would suggest that the group is interested in creating an Islamic state exclusively in the Xinjiang province ("Eastern Turkistan"), some analysts have stated that the group aims to create a new state that would include portions of Turkey, Kazakhstan, Kyrgyzstan, Pakistan, Afghanistan, and Xinjiang.

ETIM is not the only terrorist group committed to an Islamic state in the Turkistan area; the Islamic Movement of Uzbekistan (IMU) is another significant terrorist operation pushing for a theoretical Islamic Turkistan state. Claims that ETIM has ties to Al-Qaeda and the Taliban persist. Many reputable sources debate whether or not Al-Qaeda has provided the group with training and financial assistance. The US Department of State, in its 2005 report on terrorism, states that ETIM is "linked to Al-Qaeda and the international jihadist movement" and that Al-Qaeda has provided ETIM with "training and financial assistance". Another US government website reports that one ETIM leader was killed in a raid on Al-Qaeda safehouses in Pakistan.

The Chinese government, it has been suggested, has been known to exaggerate the connection between ETIM and Al-Qaeda to enlist the support of the US in endorsing China's social control tactics in Xinjiang. It is

likely that members of ETIM have had contact with Al-Qaeda elements, but no high-level contacts have been established. As far as the group's strength is concerned, ETIM has been described as a small terrorist operation and the group demonstrates limited allegiance among the ethnic Uyghurs of the Xinjiang province. Furthermore, China shows absolutely no signs of acquiescing to any of ETIM's terrorist demands. In fact, the Xinjiang province is important to China both for its strategic location and its abundant natural resources.

Chinese Black Societies

Criminal gangs are found throughout China but are most active in Chongqing, Shanghai, Macau, Tianjin, Shenyang, and Guangzhou as well as in Hong Kong and Taiwan. The number of people involved in organised crime has risen from around 100,000 in 1980 to around 1.5 million in 2000. New members are often recruited among the 120-million-strong "floating population" of migrant workers. Organised crime gangs in China are known as "black societies." The private intelligence firm Stratfor said that, unlike in Russia and Italy, organised crime was "extremely localised." Many criminals work in small, loosely-knit gangs that are involved in armed robbery, racketeering, smuggling, narcotics trafficking, prostitution, gambling and even contract murder. When groups begin to outgrow their local area, the government crack down on them heavily.

One of Henan Province's worst gangs roamed the countryside unchecked for 13 months, robbing farmhouses and killing 76 people. Seven members of the gang, including its leader Peng Miaoji, who personally cut the throat of 40 victims, were captured and executed in December 1999. Some gangs have close relations with the police and are even run by the police. In March 2007, 10 members of a police-run gang in Inner Mongolia were sentenced to up to 20 years in prison for robbery, rape, gambling and bribery. The gang had been active for more than 10 years. Whilst much of the organised crime in China is local there are exceptions and heading the list for the largest and most powerful in China as well as transnationally are the Triads, operating in China, Hong Kong, Macao, Taiwan and beyond.

Tongs - China

Tongs are similar to Triads except that they originated among early immigrant Chinatown communities independently, rather than as extensions of modern triads. The word literally means "social club," and Tongs are not specifically underground or criminal organisations. The first Tongs formed in the second half of the 19th century among the more marginalized members of early immigrant Chinese American communities for mutual support and protection. These Tongs modeled themselves on Triads, becoming involved in criminal activities such as extortion, illegal gambling, human trafficking, murder and prostitution. In recent years, some Tongs have reformed to eliminate their criminal elements and have become civic-minded organisations.

Special Focus 11

Triads - China/Hong Kong/Macau & Taiwan



China's Triads, whose history may go back as much as 2000 years, were originally secret societies. These societies grew following the overthrow of the Ming dynasty in 1644, to oppose the foreign Ch'ing (Manchu) dynasty. The term Triad is neither Cantonese nor Mandarin but was first coined by the British authorities in colonial Hong Kong, as a reference to the triads' use of triangular imagery and where membership of a triad society was prohibited and a criminal offence since 1949.

For centuries after the Triads embedded themselves in Chinese society, frequently engaging in various kinds of criminal and other illegal activity. The Triads played a major role in the Chiang Kai-shek regime gradually increasing the scope of their criminal activities, but they were enemies of the Communists and had to flee after the Communists came to power in 1949.

The Triads left settling mostly in Hong Kong, but also Macau and in Taiwan and also represented in countries with significant Chinese populations, such as Malaysia, Singapore, the US, Canada, Australia and the UK.

The Triads are considered to have more than 100,000 members and are involved in extortion, protection rackets, gun running, smuggling, fraud, drug trafficking, counterfeit goods as well as Human Trafficking but their main areas of involvement are Illegal gambling and loan sharking. Illegal gambling has long been a main stay of criminal activity for triad gangs and despite heavy police action continues to be a problem. Gambling in Hong Kong is only legal through the Hong Kong Jockey Club and only in respect of certain sporting activities.

Illegal casino, bookmaking and loan sharking operations also extend to Macau, Shenzhen and Guangdong Province. In 2001, the Hong Kong Government estimated that the annual turnover of illegal football betting alone was US\$2.5bio. Loan sharking is often connected to the Triads activities with Illegal Gambling.

A common scenario involves victims being induced to gamble more than they can afford in the VIP rooms at Macau casinos or in Illegal gambling dens. The victim is then held pending reimbursement. Family members are encouraged to make payments to free their relative,

with settlement being made by bank transfers, which are structured through a series of nominee or front accounts.

There are around 50 known Triad societies in Hong Kong, of which about 15 regularly come to Police attention, though the clandestine nature of Triad activity makes it difficult to make an accurate assessment of triad membership. Sun Yee On and 14K are the two largest and well known but other large gangs include Wo Shing Wo, Wo Hop To and Wo On Lok, which all together account for the majority of triad-related crimes in Hong Kong. Some triads or their factions operate only within a particular district and others disperse after a short time. The Hong Kong Police estimate Triad gangs are responsible for 3% of the city's crime.

Sun Yee On - China/HK

Sun Yee On or the New Righteousness and Peace Commercial and Industrial Guild, is the largest Triad gang based in Hong Kong and Mainland China, with more than 55,000 members worldwide. It is also believed to be active in the UK, the US, France, Belgium, and the Netherlands. Sun Yee On was founded in 1919.

14K - Hong Kong

The 14K is a Triad group based in Hong Kong but active internationally. It is the second largest Triad group in the world with around 20,000 members split into thirty subgroups. They are the main rivals of the Sun Yee On. The 14K are responsible for large-scale drug trafficking around the world, most of it heroin and opium from China or Southeast Asia as well as illegal gambling, money laundering, arms trafficking, prostitution, people smuggling, extortion, counterfeiting and, to a lesser extent robberies. The 14K was formed by Lieutenant-General Kot Siu-wong in Guangzhou, China in 1945 as an anti-Communist action group, relocating to Hong Kong in 1949 when the Kuomintang fled from the Communists following the Chinese Civil War. Originally there were fourteen members who were part of the Kuomintang, hence the name 14K. Compared with other Triad societies, the 14K is one of the largest and most violent Hong Kong based Triad societies, and its members appear to be more loosely connected.

Dai Huen Jai - China

The Dai Huen Jai are not a Triad gang but a Chinese criminal gang and a curious product of Mao Zedong's Cultural Revolution. On Mao's death much of the para-military Red Guard were sent to "re-education" camps, where they suffered abuse and emerged as an organised criminal syndicate involved in the same criminal activities as the Triads, i.e. drug trafficking, loan-sharking, human-trafficking, fraud, counterfeiting, prostitution, fraud, human trafficking, albeit not operating as a formal organisation but now operating in loose confederations throughout Asia, the Americas and Australia.

Taiwan

In 1895, military defeat forced China to cede Taiwan to Japan. Taiwan came under Chinese Nationalist control after World War II. Following the communist victory on the mainland in 1949, 2 million Nationalists fled to Taiwan and established a government using the 1947 constitution drawn up for all of China. Beginning in the 1950s, the ruling authorities gradually democratized and incorporated the local population within the governing structure. This process expanded rapidly in the 1980s.

In 2000, Taiwan underwent its first peaceful transfer of power from the Nationalist to the Democratic Progressive Party. Throughout this period, the island prospered and became one of East Asia's economic "Tigers." The dominant political issues continue to be the relationship between Taiwan and China, specifically the question of Taiwan's eventual status, as well as domestic political and economic reform.

Taiwan is regional transit point for heroin, methamphetamine, and precursor chemicals and a transhipment point for drugs to Japan. There is a major problem with domestic consumption of methamphetamine and heroin. Organised crime in Taiwan is dominated by Heijin gangsters, the Heavenly Alliance Gang, the Four Seas Gang and Triad groups like the United Bamboo.

Heijin - Taiwan

Taiwanese gangsters get more done when they infiltrate business or politics. A third of the government's officials are current or former members. "Heijin" which means "black gold politics" and involves the evolution of organised crime in Taiwan, turning gangsters into businessmen and some into politicians. Researchers and scholars published figures for 1996 that estimated that 106 of the more than 360 major companies in Taiwan had been infiltrated by corrupt politicians, gangsters and oftentimes both. The major organised crime gangs in Taiwan are the United Bamboo, the Heavenly Alliance Gang and the Four Seas Gang all involved in "Heijin".

United Bamboo - Taiwan

Believed to be Taiwan's top Triad gang with as many as 10,000 members, United Bamboo operates according to a decidedly old-school code of ethics that stresses unity among members as well as "harmony with the people." Although they have repeatedly denied it, United Bamboo is believed to be entrenched in drug trafficking, and their sphere of influence may even stretch into the KMT, Taiwan's ruling political party, as well as throughout Asia, the Pacific, Europe, and the Americas. Unlike other syndicates, United Bamboo is not overseen by a single boss, but rather has a more horizontal structure to its hierarchy.

Heavenly Alliance Gang - Taiwan

This Taiwanese gang came into existence in 1986 at the Taipei Detention Centre and purported to follow the spiritual leadership of Lo Fu-chu. The founding of the organisation took place in a ceremony that established branches and their respective heads, of which there were originally 6. Expansion since then has been extensive, the total number of branches swelling from 6 to 14 in 1996, and 30 in 2004. Each branch possesses a firm hierarchical structure, typically descending from the branch leader, to deputy branch leaders, advisers, unit chiefs, combat teams and members. Relationships between branches of the Heavenly Alliance are not always harmonious, the war between the new and old Sun branches being a particularly violent expression of tensions within the group. The recruitment strategy of the Heavenly Alliance is much like that of its rival Taiwanese gangs United Bamboo and the Four Seas; targeting students and school drop outs. Membership in the gang is obtained by means of a simple pledge, committing each recruit to the following four aims: i) to help heaven by dispersing justice, assisting the weak and the poor ii) to conduct oneself with honesty amongst fellow members iii) to follow the example of heaven and earth; acting with empathy and justice iv) to fly as high as possible; to extend justice around the world. The gang itself is heavily armed and commonly resorts to violence. The areas of criminal activity in which the Heavenly Alliance is most heavily committed include gambling, prostitution, debt collection, bid rigging, illegal futures trading, waste land disposal, extortion and protection rackets.

The Four Seas Gang - Taiwan

Another major organised crime gang operating in Taiwan is the Four Seas. The group is thought to have around 50,000 members and has extended its reach to some American cities. In particular the Four Seas is known to have connections with human trafficking in southern California. In terms of structural organisation the Four Seas has three primary positions of leadership at its pinnacle; those of the chairman of the committee, the deputy chairman, and the standing members of the committee. Members of the standing committee are elected by their constituent sects, or tongs, which they represent in meetings. The directives emerging from these meetings are then relayed to the separate tongs for implementation. In terms of growth the number of tongs aligned to the Four Seas has swelled from 11 in 1997 to more than 40 in 2006. A high proportion of the gang's membership is derived from school and college drop-outs, however for the most part these individuals fill periphery roles. Core roles are predominantly occupied by more long-standing criminals. Originally the gang derived its revenue from overtly criminal sources such as protection, debt collection, racketeering, prostitution, gambling, extortion and pirated merchandise. However during the 1990s the group expanded its enterprise into legal avenues. Despite this move into seemingly more legitimate commercial waters, the group continues to expand its criminal repertoire, adding credit card fraud to its long list of illegal activities.

North Korea

North Korea has a population of approximately 23 million with Pyongyang the capital and largest city. North Korea is a single-party state led by Korean Workers' Party which was chaired by the Kim's family. The country has been described by some Western countries as a totalitarian state under the dictatorship of the Kim's family and has long been criticized for its lack of political and human rights. North Korea is one of the poorest countries in Asia, but still maintains one of the world's largest armies totaling 9,495,000 active, reserve, and paramilitary personnel, a hangover from the Korean war which ended in a stalemate in 1953. Korea was occupied since 1910 by Japan and divided in two by the World War 2 allied victors along the 38th parallel. The North invaded the South in 1950 which was rebutted by a UN force that led to an armistice 3 years later after bitter fighting and after China joined the war in support of the North.

In 1987 North Korean agents placed a bomb on [Korea Air Flight 858](#) killing 115. It is a nuclear-weapons state and has an active space programme, despite regularly having to rely on international food aid to feed its citizens. In 2006 in an attempt to persuade North Korea from developing nuclear weapons, UN, EU, US and other Western countries imposed various economic sanctions, such as a military and trade embargo, though the regime was still able to avoid restrictions to build its nuclear programme largely by working with the Proliferation network built by [Abdul Qadeer Khan](#). For more information see Part 1, Section 3, Money Laundering Laws and Regulations, Sanctions and Embargoes above.

According to a report released by a UN experts panel in July 2012, North Korea continues to violate UN sanctions by attempting to ship arms to Syria and Burma and illegally importing luxury goods. The Financial Action Task Force (FATF) issued a public statement on 16 February 2012 listing countries around the world which have significant deficiencies in their anti-money laundering regulations, one of which was North Korea. According to the FATF, the government of North Korea has repeatedly failed to take adequate steps in addressing serious shortcomings in the fight against money laundering and terrorist financing. FATF called on all its member countries to apply new counter-measures to protect national and international businesses from the continued and substantial risk of money laundering stemming out of North Korea. Corruption is widespread in North Korean society. North Korea is ranked 181 out of 182 countries in Transparency International's 2011 Corruption Perceptions Index. Whilst much of the nation lives in poverty and many require food aid, Kim Jung-Un, who succeeded Kim Jong-il in 2011, enjoys a luxurious lifestyle, allegedly he smokes Yves Saint Laurent cigarettes and loves Johnnie Walker whiskey and has a Mercedes-Benz 600 Sedan, rides horses and enjoys riding jet skis and imports consumer goods

like large screen TVs and other consumer electronics. According to a South Korean Parliamentary Report, the communist country's inbound shipments of luxury goods amounted to US\$322.5mio in 2009 before rising to US\$446.2mio in 2010 and US\$584.8mio in 2011. In addition to some legitimate exports and trade it is believed that the North Korean State is blatantly involved in criminal activity, in drug production and trafficking, initially opium and now meths, currency counterfeiting and arms dealing.

South Korea

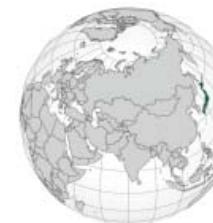
In the city of Seoul, South Korea is the local district of Gangnam, which means "South of the River". As of September 2013 the eponymous pop video 'Gangnam Style' had been viewed over 1.7 billion times.

The phrase 'Gangnam Style' is Korean term for someone enjoying a lavish lifestyle and is being used in a country that when the UN Secretary General, Mr Ban Ki-Moon was aged 6, at the beginning of the Korean War, was a byword for desolation and poverty. The name Korea is derived from the Goryeo dynasty which ruled in the middle ages. Its recent history involved conquest by Japan, then liberation followed immediately by being the battleground for the only "hot" war within the 'cold war'. One that involved the USA, USSR, China and others. In South Korea's early years it enjoyed virtually continuous economic growth even though it wasn't till 1987 that Civilian rule became the norm. Even today it has the world's most fortified border and the second highest number of soldiers per capita in the world. North Korea has the highest.

Criminal gang members in South Korea are known as Khangpae, literally meaning 'thug'. Criminal syndicates control large parts of South Korea's media, entertainment and even political activities. Today the two main criminal syndicates are the Seven Star Mob, and the HSS MOB. Another, the Double Dragon Mob has declined or gone underground. The HSS Mob is known to have links with Japanese, Brazilian, Chinese, US and Mexican gangs. Drugs, racketeering, prostitution and protection rackets form the main activity. Human Trafficking is an obvious adjunct to their overseas prostitution activities whilst money laundering has grown through the cover of construction businesses and gambling. They have also increasingly become part of legitimate business organisations.

Corruption is by any measure endemic in South Korea. Annually named and shamed by Transparency International, the criticism has also come from the Political and Economic Risk Consultancy's 2013 Report on Corruption in Asia which said that 'Korea is the most corrupt amongst developed nations in Asia'. The report also said that "the roots of corruption in Korea stretch to the highest levels of government and business".

Japan



Settled by migrants from the Asian mainland back in the mists of prehistory, Japan has seen the rise and fall of emperors, rule by samurai warriors, isolation from the outside world, expansion over most of Asia, defeat and rebound. One of the most war-like of nations in the early twentieth century, today Japan often serves as a voice of pacifism and restraint on the international stage.

The word "Japan" is commonly believed to have originated from Italian traveller Marco Polo (1254-1324) who described it in his book, "Il Milione". He called the country Cipangu, and this is said to be the origin of the word Japan (or Giappone in Italian, Japon in French, etc...), and is thought to be the name for Japan used in China, where Marco Polo picked up the name.

In 1603, after decades of civil warfare, the Tokugawa shogunate (a military-led, dynastic government) ushered in a long period of relative political stability and isolation from foreign influence. For more than two centuries this policy enabled Japan to enjoy a flowering of its indigenous culture.

Japan opened its ports after signing the Treaty of Kanagawa with the US in 1854 and began to intensively modernise and industrialise.

During the late 19th and early 20th centuries, Japan became a regional power that was able to defeat the forces of both China and Russia. It occupied Korea, Formosa (Taiwan), and southern Sakhalin Island.

In 1931-32 Japan occupied Manchuria and in 1937 it launched a full-scale invasion of China. The Japanese forces succeeded in occupying almost the whole coast of China and committed severe war atrocities on the Chinese population, especially during the fall of the capital Nanking. However, the Chinese government never surrendered completely and the war continued on a lower scale until 1945. In 1940, Japan occupied French Indochina (Vietnam) with the agreement of the French Vichy government and joined the Axis powers, Germany and Italy. These actions intensified Japan's conflict with the US and Great Britain which reacted with an oil boycott. The resulting oil shortage and failures to solve the conflict diplomatically made Japan decide to capture the oil rich Dutch East Indies (Indonesia) and to start a war with the US and Great Britain. To this end, Japan attacked US forces in 1941, triggering America's entry into World War II and soon occupied much of East and Southeast Asia.

On 27 July 1945, the Allied powers requested Japan in the Potsdam Declaration to surrender unconditionally, or destruction would continue. The ultimatum was rejected, leading to the dropping by US forces of two atomic bombs on Hiroshima and Nagasaki on August 6 and 9, and the Soviet Union entered the war against Japan on August 8. After its defeat in World War II, Japan recovered to become an economic power and an ally of the US and EU. While the emperor retains his throne as a symbol of national unity, elected politicians hold actual decision-making power.

Following three decades of unprecedented growth, Japan's economy experienced a major slowdown starting in the 1990s, but the country remains a major economic power. Japan is one of the most technologically advanced societies on earth; as a result, it has the world's third largest economy by GDP (after the US and more recently China).

Japan is home to about 127.5 million people. Today, the country suffers from a very low birth rate, making it one of the most rapidly aging societies in the world. The Yamato Japanese ethnic group comprises 98.5% of the population, with the others largely made up from Koreans (0.5%) and Chinese (0.4%), as well as the indigenous Ainu people, and an estimated 360,000 Brazilians and Peruvians of Japanese origin have also returned to Japan. 95% of Japanese citizens adhere to a blend of Shintoism and Buddhism.

The Japanese Archipelago includes more than 3,000 islands, covering a total area of 377,835 square kilometers. The four main islands, from north to south, are Hokkaido, Honshu, Shikoku, and Kyushu. Japan is largely mountainous and forested, with only 11.6% of its area arable land.

Japan has avoided mostly the attentions of terrorists, with the exception of the Japanese Red Army which was a communist militant group active in 1971 but largely closed down by 1972. The most widely reported attack by terrorists was carried out in 1995 with the Tokyo subway sarin attack, (5,500 injured, 12 dead), attributed to the cult [Aum Shinrikyo](#).

The most significant organised crime threat in Japan comes from the [Yakuza](#), with the largest [Yakuza](#) gangs in Japan today joined together in large syndicates. In Japan there are three main syndicates: the [Yamaguchi-gumi](#) (headquartered in Kobe), the [Sumiyoshi-kai](#) (Tokyo) and the [Inagawa-kai](#) (Tokyo). The dominance of these three syndicates has grown steadily since the 1970s and today they account for nearly three-quarters of the [Yakuza](#) population.

The [Yakuza](#) pursue money and power through extortion, intimidation, fraud, corruption, and a remarkably diverse range of criminal or near-criminal activities. Their main businesses are drug-dealing, smuggling, prostitution, gambling, and protection rackets. The two most

serious threats that the Yakuza pose to Japanese society today are their potential to disrupt the mainstream business world through corporate frauds and extortion rackets, and their harassment of the general public through loan-sharking, aggressive debt-collecting.

Two trends in Yakuza operations are apparent: a shift from traditional rackets toward white collar crime, and a shift from consensual activities (such as gambling and prostitution) toward more predatory activities (such as loan-sharking and theft).

While the latter problem is responsible for turning public opinion against the Yakuza, it is concern about Yakuza infiltration of the business world, and of the finance sector in particular, that has been the primary galvanizing factor behind the anti-Yakuza measures implemented over the last two decades.

Japanese Red Army - Japan

The Japanese Red Army was founded by Fusako Shigenobu in Japan in 1971 and attempted to overthrow the Japanese government and start a world revolution. Allied with the Popular Front for the Liberation of Palestine (PFLP), the group committed assassinations, hijacked a commercial Japanese aircraft, and sabotaged a Shell oil refinery in Singapore. On 30 May 1972, Kōzō Okamoto and other group members launched a machine gun and grenade attack at Israel's Lod Airport in Tel Aviv, killing 26 people and injuring 80 others. Two of the three attackers then killed themselves with grenades.

Aum Shinrikyo / Aum Supreme Truth - Japan

A religious cult with goals to rule the world was established in 1987 by Shoko Asahara, with up to 9,000 members in Japan and up to 40,000 worldwide, including in Australia, Russia, Ukraine, Germany, Taiwan, Sri Lanka, the former Yugoslavia, and the US, made its move in 1995 by attacking the Japanese subway.

In March 1995 Aum members simultaneously released the chemical nerve agent sarin on several Tokyo Subway Trains, killing 12 people and causing up to 6,000 to seek medical treatment. Subsequent investigations by the Japanese government revealed the group was responsible for other mysterious chemical incidents in Japan in 1994, including a sarin gas attack on a residential neighborhood in Matsumoto that killed seven and hospitalised approximately 500. Japanese police arrested Asahara in May 1995. He was charged convicted and paid the price when the death penalty was imposed and carried out in October 2007. Although Aum has not conducted a terrorist attack since 1995, concerns remain regarding its continued adherence to the violent teachings of founder Asahara that led AUM to carry out the 1995 sarin gas attack. Today the group still has members in Japan with a residual branch of about 200 followers who live in Russia.

Special Focus 12

Yakuza - Japan



Yakuza is the name given to organised criminal gangs from Japan. The Japanese police, call them bōryokudan literally "violence group", while the Yakuza call themselves "ninkyō dantai" "chivalrous organisations". The Yakuza are notoriously known for their strict codes of conduct and very

organised nature. They are very prevalent in the Japanese media and operate internationally with an estimated 100,000 members.

Yakuza are involved in Illegal gambling and prostitution as well as the smuggling of banned goods such as drugs and firearms. The Yakuza though are most well known for extortion or protections rackets, in which Yakuza threaten business owners and other citizens with violence unless they pay up. They even target large, listed Japanese Companies. In addition to illegal markets Yakuza also have interests in real estate, construction and entertainment. Japan's professional wrestling leagues and venues are particularly known for Yakuza involvement.

The Yakuza's most direct ancestors are groups of quasi-legal businessmen from the 18th century who gambled or peddled goods on the streets of large cities. Known as bakuto and tekiya, respectively, these gamblers and peddlers still lend their names to some Yakuza clans today. These groups gradually organised themselves into gangs known as families or clans, which had formal hierarchies and rules.

In the late 19th century, the Yakuza became associated with nationalist, militaristic ideologies and politics. Gangs cultivated alliances with politicians, and politicians used them to assassinate opponents, strong-arm trade groups or even fight in nearby nations like China. The disorder of post-World-War-II Japan may also have given the Yakuza an even stronger foothold in Japanese economics and politics.

The Yakuza is not a single organisation but rather a collection of separate gangs or clans akin to the American Mafia. These violent criminals have left their fingerprints on many aspects of Japanese life, from lowly gambling and prostitution rackets to the halls of high-level political and financial power.

The various gangs that make up the Yakuza have different origins, and the gangs' versions of these origins can

be quite different from the historical record. In their own vision of themselves, Yakuza descend from honorable, Robin-Hood-like characters who defended their villages from roving bandits. Some even claim to trace the Yakuza's lineage to Ronin, samurai warriors who found themselves without masters following a period of political upheaval in 17th century Japan.

Others claim that Yakuza instead originated with the kabuki-mono, "the crazy ones." These were wildly-dressed hoodlums who carried very long swords, intimidated entire villages and sometimes executed civilians for no particular reason. The truth is likely a blend of the two stories. Left without a military hierarchy to give their lives focus, many samurai turned to crime. Others moved into merchant trades or shadier businesses such as gambling houses and brothels. These criminals, master-less warriors and newcomers to the Japanese market system had one thing in common: they were all outsiders.

The name "Yakuza" reflects this outsider status. It comes from a Japanese card game called Oicho-Kabu. This game is similar to baccarat in that the point value of a hand is based on the final digit of the hand's score. A hand of eight, nine and three equals 20, which is worth zero points - the worst possible hand in the game. The Japanese words for eight, nine and three (ya, ku and za) became the word "Yakuza," meaning worthless or pointless.

A Yakuza family has a structure superficially similar to a Mafia family. A single patriarch rules the clan. He has various lieutenants, under-bosses and minor gang leaders beneath him in a roughly pyramidal structure. Regional leaders, assistants, advisers and an assortment of thugs further complicate the Yakuza clan structure. Some clans have a different structure -- they act as broad alliances that bring many smaller gangs under one umbrella.

The key to the hierarchy is the oyabun-kobun relationship, a set of father-son roles that binds all Yakuza clans together. In return for absolute loyalty and unquestioning obedience from his kobun, the oyabun provides advice and guidance along with protection and prestige. The focus on honor and tradition in Japanese society further cements these relationships. It also doesn't hurt that the punishments for failing the oyabun range from the humiliating (expulsion from the clan) to the gruesome (cutting off part of a finger). Each member of the clan may play both the oyabun and the kobun roles, acting as a subordinate to the Yakuza immediately above him and as a boss to the gangsters below him.

Entry into both an oyabun-kobun relationship and a Yakuza clan is marked by a special ceremony. A third person pours glasses of sake for the new member and his oyabun boss. The boss and new member drink some of the sake from their own glasses. Then, they exchange glasses and drink some of each other's sake. The boss

drinks his fill while the initiate merely sips.

Although many Yakuza clans have nationalistic ideologies, Koreans have a strong presence within the Yakuza. Koreans are sometimes looked down upon in Japanese society, which feeds into the Yakuza's outsider status. The profitability of smuggling goods between Japan and Korea also contributes to this Korean influence. Women are marginalized by the Yakuza. Even the daughters and wives of clan members tend to be little more than servants at best, and they're sometimes used as gang prostitutes.

Yakuza participate in many of the same money-making activities as all criminal gangs. Illegal gambling and prostitution are Yakuza hallmarks, while the smuggling of banned goods such as drugs, firearms and pornography is also profitable. The age-old protection racket, in which Yakuza threaten business owners and other citizens with violence unless they pay a tribute, is a common Yakuza tactic as well.

Japanese gangsters also operate legal businesses using the profits from the illegal ones. Real estate, construction and entertainment are all industries in which Yakuza have become involved. Japan's professional wrestling leagues and venues are particularly known for Yakuza involvement.

Higher-level Yakuza often play the Japanese stock market, sometimes legally. They may also find or invent incriminating information about a company and use this information to blackmail its board of directors. After buying shares of the company's stock, a clan sends some of its members to board meetings, where they threaten company officials with the release of the evidence. Yakuza can exert a great deal of control over businesses this way or simply demand payoffs.

Many Yakuza extortion and blackmail schemes are carefully designed to maintain the Japanese tradition of politeness. Yakuza may ask corporations to attend golf tournaments, give to fake charities or purchase certain items, all at ridiculously inflated prices. The corporations' leaders know that there is an implied threat with such requests, so they often go along even though the Yakuza never make a direct threat or demand.

Yubitsume, or the cutting of one's finger, is a form of penance or apology. Upon a first offence, the transgressor must cut off the tip of his left little finger and hand the severed portion to his boss. Sometimes an underboss may do this in penance to the oyabun if he wants to spare a member of his own gang from further retaliation. Its origin stems from the traditional way of holding a Japanese sword. The bottom three fingers of each hand are used to grip the sword tightly, with the thumb and index fingers slightly loose. The removal of digits starting with the little finger moving up the hand to the index finger progressively weakens a person's sword grip. The idea is that a person with a weak sword grip then

has to rely more on the group for protection—reducing individual action. In recent years, prosthetic fingertips have been developed to disguise this distinctive appearance.

Many Yakuza have full-body tattoos. These tattoos, known as irezumi in Japan, are still often “hand-poked”, that is, the ink is inserted beneath the skin using non-electrical, hand-made and hand held tools with needles of sharpened bamboo or steel. The procedure is expensive and painful and can take years to complete. When Yakuza members play Oicho-Kabu cards with each other, they often remove their shirts or open them up and drape them around their waists. This allows them to display their full-body tattoos to each other. This is one of the few times that Yakuza members display their tattoos to others, as they normally keep them concealed in public with long-sleeved and high-necked shirts. When new members join, they are often required to remove their trousers as well and reveal any lower body tattoos.

Although Yakuza membership has declined following an anti-gang law aimed specifically at Yakuza and passed by the Japanese government in 1992, there are thought to be more than 103,000 active Yakuza members in Japan today. Although there are many different Yakuza groups, together they form the largest organised crime group in the world.

Yamaguchi-gumi - Japan

The Yamaguchi-gumi was established in 1915 and is the biggest Yakuza family, accounting for 50% of all Yakuza in Japan, with more than 55,000 members divided into 850 clans. Despite more than one decade of police repression, the Yamaguchi-gumi has continued to grow. From its headquarters in Kobe, it directs criminal activities throughout Japan. It is also involved in operations in Asia and the US. Shinobu Tsukasa, also known as Kenichi Shinoda, is the Yamaguchi-gumi's current oyabun who took over in 2005 albeit Kiyoshi Takayama was in de facto control until recently until he too was imprisoned on extortion charges. Its success can be largely attributed to the organisation's long time oyabun, Kazuo Taoka who was seen and still regarded as an ultra-violent venerated mastermind of the group. Whilst based in Kobe, the group has expanded throughout Japan including in Tokyo.

Sumiyoshi-kai - Japan

The Sumiyoshi-rengo is the second largest Yakuza family, with 20,000 members divided into 277 clans. The Sumiyoshi-kai, as it is sometimes called, is a confederation of smaller Yakuza groups. Its current oyabun is Shigeo Nishiguchi. Structurally, Sumiyoshi-kai differs from its principal rival, the Yamaguchi-gumi, in that it functions like a federation. The chain of command is more lax, and although Shigeo Nishiguchi is always the supreme oyabun, its leadership is distributed among several other people.

Inagawa-kai - Japan

The Inagawa-kai is the third largest Yakuza family in Japan, with roughly 15,000 members divided into 313 clans. It is based in the Tokyo-Yokohama area and was one of the first Yakuza families to expand its operations to outside of Japan. Its current oyabun is Hideki Inagawa. Members often wear sunglasses and colourful suits so that their profession can be immediately recognised by civilians (kataji). Even the way many Yakuza walk is different from ordinary citizens. Their wide gait is markedly different from the unassuming way many Japanese prefer. Alternatively, Yakuza can dress more conservatively and flash their tattoos to indicate their affiliation when the need arises. On occasion, they also sport insignia pins on their lapels.

Dojin-kai - Japan

A Yakuza family centring its operations on the Japanese island of Kyushu, the Dojin-kai has become renowned for its drug trafficking, especially in methamphetamine. This is a sector that the Dojin-kai are alleged to have dominated in Japan since the late twentieth century. The Dojin-kai have also built a reputation for violent conduct in their affairs, exacting bloody vengeance on the Kyushu Seido-kai in particular for their defection. Today the group is believed to be led by Seijiro Matsuo.

Kyushu Seido-kai - Japan

Another Yakuza family based on the Japanese island of Kyushu, the group is believed to have 380 active members. The Kyushu Seido-kai originated as a splinter group of the Dojin-kai Yakuza family in 2006 and now forms one of five Yakuza syndicates based in the Fukuoka prefecture of Kyushu. An ongoing feud exists between the Kyushu Seido-kai and the Dojin-kai, resulting in the death of several Seido members. The Kyushu Seido-kai is characterised by its loan-sharking and drug trafficking operations, specialisations learnt during their time as part of the Dojin-kai's drug trading wing. As a result the Seido-kai are sometimes known informally as the ‘Seido Pharmacy’.

Central Asia



Central Asia is a core region of the Asian continent which stretches from the Caspian Sea in the west to China in the east, Afghanistan in the south, and Russia in the north. It is also sometimes referred to as Middle Asia, and, colloquially, “the stans” (as the five countries generally

considered to be within the region all have names ending with that suffix) and is within the scope of the wider Eurasian continent.

In modern contexts, all definitions of Central Asia include these five republics of the former Soviet Union: Kazakhstan (pop. 16.0 million), Kyrgyzstan (5.5 million), Tajikistan (7.3 million), Turkmenistan (5.1 million), and Uzbekistan (27.6 million), for a total population of 61.5 million as of 2009. Other areas often included are Mongolia, Afghanistan, northern Pakistan, northeastern Iran, Kashmir, and sometimes Xinjiang and Tibet in western China and southern Siberia in Russia. During pre-Islamic and early Islamic times, Central Asia was a predominantly Iranian region that included sedentary Sogdians, Chorasmians, semi-nomadic Scythians and Alans. The ancient sedentary population played an important role in the history of Central Asia. After expansion by Turkic peoples, Central Asia also became the homeland for many Turkic peoples, including the Kazakhs, Uzbeks, Turkmen, Kyrgyz and Uyghurs.

Central Asia is sometimes referred to as Turkestan. Since the collapse of the Soviet Union and the discovery of Gas, Oil, Gold and other Metals its strategic importance is becoming more and more recognised. Three of the Central Asian states border Afghanistan. Notwithstanding the conflict in Afghanistan the USA, Russia and India also have military bases in the Central Asian Republics. It is however of more specific strategic concern because of its proximity to Afghanistan which, aside from the current conflict there, has a near monopoly on the production of the world's opiate drugs; much of which passes through Central Asia on its way to Russia and Western Europe.

Many official views of governance in the Central Asian Republics are at best ‘diplomatic’ suggesting that these States are at the very early stages of transition from personal fiefdoms to democracies. In some alternative accounts they are described as vicious, corrupt, kleptocracies. The reality is that the Central Asia Republics are characterised by de facto dictatorships, (some benign some not so) who are in varying degrees accused of nepotism, corruption and the repression of press and

political freedom, amongst many other things.

The Economist Intelligence Unit produces a Democracy Index and the Central Asian Republics featured in 2011 as follows: Kyrgyzstan 107, Kazakhstan 137, Tajikistan 149, Uzbekistan 164, and Turkmenistan 165. As a comparator the lowest, North Korea, is at 167. Other Indices such as the Corruption Perception Index mirror the poor scoring for democracy, similarly the Press Freedom Index.

Transnational organised crime in Central Asia represents a serious threat to the region. Criminal organisations from Central Asia are often inaccurately described as part of the Russian Mafia. In fact they may use the Russian language, which is the lingua franca of the region, but they are very much a product of their own clans and tribes (or Hordes). As an example clans from the Great Horde dominate the Kazakhstan government. These tribal and clan structures go back many generations with family and clan relations serving as powerful organizing structures that can often be conducive to corruption – both for government personnel and organised criminals.

In 2007 an UNODC Report created a typology of Central Asian criminal groups which showed 6 categories which whilst it neatly classified these groups, the utility of that classification is only for academics. It did show however the sheer complexity of combating such groups and the adaptability and flexibility of their organisations, some of which though very insular have still formed links with other national and transnational organised crime groups.

According to the US State Department, there is significant evidence of organised crime in Kazakhstan. Many organised crime groups are also reported to have ties with similar groups in the US and Europe, Central Asia has also become an increasingly important area for illicit armaments trafficking linked to the conflict in Afghanistan. Human Trafficking is also a large and growing problem.

The UNODC reported that, according to the Kazakh authorities, the Izmailov organisation based in Moscow, along with Chechen and Ingush organisations and members of the Slavic “Thieves-in-Law” have attempted to re-establish the criminal tradition, of the “thieves’ code”, in Kazakhstan. Thieves in law are the elites of the post-Soviet era of organised crime and they formed as a society as a result of ruling the criminal underworld within the prison camps and are otherwise known as the ‘vory’. Other reports show inter-regional and international links being made with other organised criminal groups

Drug Trafficking is the main area of organised crime in Central Asia. The region with its porous borders acts as trans-shipment area for the so called “Northern Route” passing through its states for Russia and Western Europe. The International Narcotics Control Board

has estimates that 20% of the opiates coming out of Afghanistan pass through the Central Asia countries. US State Dept Narcotics Report 2012 mentions CAR states on the transshipment route, stating that "Afghan opiates pass through Kyrgyzstan's borders with Tajikistan, Uzbekistan, and Kazakhstan. The Kyrgyz Republic faces serious problems in monitoring its borders due to the topography of the country, of which 94% is mountainous." In addition, "one hundred thousand hectares of wild-growing cannabis in the country serve as a raw product source for local criminals for production of marijuana and hashish.

Central Asia is a transit point for illegal immigrants, in particular from South Asia..

Today, all countries in the C.A.R. States are either an origin, transit or destination point for trafficked children, some are all. Some trafficking is internal or cross border and often for labour use. Trafficking for sexual purposes exists and each state has laws to protect children but the problem is simply that children are at the bottom of the list for state help. Once again the litany of poverty, corruption, and organised crime leads inevitably to a degree of societal breakdown that worse affects the most vulnerable. Child prostitution and child pornography represent a lucrative area of business for organised criminal groups.

Arms' trafficking in Central Asia is linked to trafficking in drugs. For example, in Tajikistan, drug trafficking has been used for funding firearms purchases; with opposition militants buying drugs from Afghanistan, selling them in the Russian Federation and then returning to Afghanistan to purchase weapons. There is also a fear that various ethnic groups may be setting up arms dumps in anticipation of possible inter-ethnic conflict, particularly in the Ferghana valley, which stretches across Eastern Uzbekistan, Kyrgyzstan and Tajikistan. Islamist Groups such as Hizb ut-Tahrir are also one of several Islamist groups in the region. All smugglers however are armed and willing to use them thus exacerbating the porosity of borders. Border guards in any case are often priced into the transit costs of any goods whether goods, persons or cash.

The C.A.R States, like their Soviet predecessors, are concerned about the rise of Islamic groups some of whom have become radicalized and show an increasing capability of staging attacks. The main current terrorist threat in the C.A.R states is to Tajikistan which has a growing threat of insurrections both internally and externally. The main opposition party the Islamic Renaissance Party is alleged to be becoming more radicalised.

In fact all the classic hallmarks of creating dissent are there. In 2011 Tajik security forces were forced to make a temporary peace with warlords and insurgents in the eastern Rasht district who wish to see an Islamist Caliphate.

This peace is coming to an end and there is now a resurgence of the Islamic Movement of Uzbekistan (IMU), a group that is fighting in Afghanistan along with the Taliban. It is feared that many of the fighters in Afghanistan are closely linked to the IMU and will eventually turn their attention from Kabul to Tajikistan. On its own Tajikistan has virtually no capacity to control the 900 mile Tajik-Afghan border and the existing state apparatus is not strong enough to combat an insurgency. China will not want any insurgency to spread to the Uighurs in China or the Russians see it connect to the Caucasus. Pakistan will want to support its Sunni co-religionists but Iran will want to support its Shia brethren. The main terrorist threats in the region come from the Islamic Movement of Uzbekistan, and its offshoots or affiliates Hizb ut-Tahrir al-Islami, Hizb-an-Nusra; Akromiya; Jama'at al-Jihad al-Islami also known as the Jamaat of Central Asian Mujahideens (JCAM), and Islamic Jihad Group (IJG), all of whom are seen as Islamic terrorist organisations affiliated with Al-Qaeda that operates in the CAR region, being dedicated Other groups mentioned as relevant also include, the Kurdistan Workers Party, Lashkar-e-Toiba, Aum Shinrikyo and the East Turkestan Liberation Organisation. These Organisations are banned in one or more of the CAR states.

One of the worst terrorist attacks occurred in 2004 in Tashkent, Uzbekistan, when suicide bombers killed 47 people. The Islamic Movement of Uzbekistan, an organisation affiliated with Al-Qaeda and Islamic Jihad claimed responsibility. Uzbek President, Islam Karimov claimed the perpetrators were ex-members of Hizb-ut-Tahrir.

Uzbekistan

Russia conquered the territory of present-day Uzbekistan in the late 19th century, later establishing a socialist republic in 1924. During the Soviet era, intensive production of "white gold" (cotton) and grain led to overuse of agrochemicals and the depletion of water supplies, leading to significant degradation of the Aral Sea. Independent since 1991, the country is ruled by President Islam Karimov and borders Afghanistan which allows for narcotics, money and other goods to enter and pass through the country. Corruption, narcotics trafficking, and smuggling generate the majority of illicit proceeds. Local and regional drug trafficking and other organised criminal gangs control narcotics markets and proceeds from other criminal activities, such as smuggling of cash, gold, precious stones. Current concerns also include terrorism by Islamic militants.

Islamic Movement of Uzbekistan (IMU) - Afghanistan/Pakistan

The Islamic Movement of Uzbekistan's was designated as a US Foreign Terrorist Organisation on 25 September 2000. The Islamic Movement of Uzbekistan's goal is to overthrow the Uzbek regime and establish an Islamic

state. For most of the past decade, however, the group recruited members from other Central Asian states and Europe and has focused on fighting in Afghanistan and Pakistan. The IMU has a relationship with the Taliban and Tehrik-e Taliban Pakistan (TTP).

In 2011, IMU's leadership cadre remained based in Pakistan's Taliban-controlled North Waziristan and operated primarily along the Afghanistan-Pakistan border and northern Afghanistan. Top IMU leaders have integrated themselves into the Taliban's shadow government in the northern provinces. Operating in cooperation with each other, the Taliban and the IMU have expanded their presence throughout northern Afghanistan and established training camps in the region. Since the beginning of Operation Enduring Freedom, the IMU has been predominantly focused on attacks against US and Coalition soldiers in Afghanistan. In late 2009, NATO forces reported an increase in IMU-affiliated foreign fighters in Afghanistan. In 2010, the IMU continued to fight in Afghanistan and they claimed credit for the 19 September ambush that killed 25 Tajik troops in Tajikistan. On 15 October 2011, IMU claimed responsibility for a suicide assault on a US-led Provincial Reconstruction Team base in the Afghan province of Panjshir. The attack began when a suicide bomber detonated a car packed with explosives at the front gate, killing two Afghan civilians and wounding two security guards at the base. The IMU receives support from a large Uzbek diaspora, terrorist organisations, and donors from Europe, Central and South Asia, and the Middle East.

For details of other groups agitating in the region see Middle East Sections and in East Asia Sections above concerning East Turkestan.

Islamic Jihad Group - Uzbekistan

The Islamic Jihad Group (IJG) is a violent terrorist organisation responsible for several high-profile bombings in Uzbekistan. Islamic Jihad Group is a splinter organisation from the Islamic Movement of Uzbekistan (IMU).

The IJG was previously unknown until April 2004 when the group claimed responsibility for a series of suicide bombings around Tashkent and Bukhara, which killed 47 people. The attacks targeted local government offices, as well as a crowded market. Although IJG released a statement claiming responsibility for the bombings, officials doubted the existence of the unknown group, and blamed other extremist organisations. On 30 July 2004, IJG carried out simultaneous bombing attacks on the US Embassy, the Israeli Embassy, and the Uzbek Prosecutor General, killing at least two people and wounding several. The attacks were highly sophisticated, and they cemented IJG's status as a real terrorist threat in Central Asia. In their claim of responsibility, the IJG wrote: "A group of young Muslims executed martyrdom operations that put fear in the apostate government and its infidel allies, the Americans and Jews. The Mujahideen belonging to Islamic Jihad Group attacked both

the American and Israeli embassies as well as the court building where the trials of a large number of the brothers from the Group had begun. These martyrdom operations that the group is executing will not stop, God willing. It is for the purpose of repelling the injustice of the apostate government and supporting the jihad of our Muslim brothers in Iraq, Palestine, Afghanistan, the Hijaz, and in other Muslim countries ruled by infidels and apostates."

Although IJG has not publicly elucidated their goals and philosophy, from their background and statements it is clear that they are deeply opposed to the current authoritarian-secular rule in Uzbekistan, and wish to set up an Islamic state in its place. Besides being closely linked with IMU, many officials speculate that IJG has close ties to Al-Qaeda given the sophisticated nature of their attacks and targets. The IJG has been designated as a terrorist organisation first by the US in 2005.

Kazakhstan

Ethnic Kazakhs, a mix of Turkic and Mongol nomadic tribes who migrated into the region in the 13th century united as a single nation, before Russia was conquered in the 18th Century, and Kazakhstan became a Soviet Republic in 1936. Since the break up of the Soviet Union and independence Kazakhstan has had one person one party rule under Nursultan Nazarbayev, who assumed leadership of the Soviet Republic, siding with Boris Yeltsin and so able to secure his authority which remains to this day.

Timur Kulibayev is the son-in-law of the President of Kazakhstan marrying Dinara Nazarbayeva and has been for some time seen as the heir apparent to the President. Kulibayev plays a prominent role in the business world, having held a number of commanding positions in the Kazakh economy, including the chairmanships of the sovereign wealth fund, (Timur Kulibayev resigned from the post of Chairman of the Board of Samruk-Kazyna after riots in 2011), the national oil and gas company, and the national railway company. Kulibayev also sits on the board of Russian state-owned energy giant Gazprom. Leaked US diplomatic cables alleged that Timur Kulibayev was the "ultimate controller of 90%" of Kazakhstan's economy.

Kazakhstan's economy is larger than those of all the other Central Asian states largely due to the country's vast natural resources.

Kazakhstan is a producer of cannabis for CIS markets, as well as limited cultivation of opium poppy and ephedra (for the drug ephedrine) and a transit point for Southwest Asian narcotics bound for Russia and the rest of Europe as well as a significant consumer of opiates. Governmental corruption, an organised crime presence and a large shadow economy make the country vulnerable to money laundering and terrorist finance.

Oceania



Oceania includes all the islands of the South Pacific, divided into the subregions of Melanesia, Micronesia, and Polynesia as well as Australasia and in some definitions even Malaysia, but in others not. Whilst Australia is the largest country in the region, itself being the 6th largest in the World with a population of just over 20 million, the region itself is made up of 14 Countries in all and 25 dependencies and home to more than 35 million people. Oceania was named after the pacific ocean which surrounds it in 1812 by French geographer Conrad Malte-Brun and is derived from the french word Océanie. Micronesia is the northern most region of Oceania, parallel to the Philippines, including Kiribati and the Marshall Islands. Melanesia is directly south of Micronesia and includes New Guinea, Vanuatu, Fiji and the Solomon Islands. Polynesia is west of both Micronesia and Melanesia and includes Tonga, the Marshall Islands Guam and Easter Islands, Tuvalu and the Cook Islands. Australasia is usually considered to include both Australia and New Zealand, though some definitions will include also New Guinea and nearby islands and in some other definitions New Zealand is also considered part of Polynesia.

Australia

Clearly the economic dominance of Australia in the region would also suggest predominance in organised crime. Transnational gangs are involved in common activities such as drugs but demonstrate an ability to enter into new illicit activities. As is often the case world wide, gangs in Australia often form on ethnic lines, and there are Chinese Triads, Japanese Yakuza and Vietnamese gangs, but also include Lebanese, Italian, Romanian and even Colombian Syndicates. Of the Triad groups the 14K is well established in Sydney with branches in the other major cities. Also active are the Big Circle syndicate. In Melbourne as well as those already mentioned are the Sun Yee On and the Wo Yee Tong and the Wo Shing Wo. The latter two are sub-groups of the Wo Group. These gangs are active in blackmail, extortion, and illegal gambling as well as the ubiquitous heroin imports. Vietnamese groups have now grown substantially and include armed robbery and heroin distribution in their repertoire. The Australian Federal Police have for several years campaigned against The Yakuza whom it is felt are trying to become established in Queensland. The presence of Italian gangs in Australia is that of a national network of family relationships and areas of mutual interest rather than some sort of Mafia style organisation. They are mainly involved in the growing of cannabis but

some are expanding into the importation and distribution of heroin and cocaine. As a consequence they are also involved in money laundering. On a smaller scale the same could be said for the Lebanese except that they import hashish and heroin from Lebanon. Romanian groups are importing small but significant amounts of heroin and have been involved in social security frauds. The Colombian Cartels use Australia as a transit country for drugs and there is increasing evidence that the country has a laundering function for them as well. There are also worrying signs that they are steadily expanding by increased links to other groups and organically in their own right. Most of the cannabis and amphetamines consumed are also produced within Australia, whilst heroin comes from the Golden Triangle countries and cocaine from South America. Sydney is the main gateway for imported drugs. The immensely long coastline of Australia is clearly not easy to police and shipping, particularly container shipping is increasing all the time. Asian groups are particularly specializing in markets like heroin and are now known to be able to corrupt public and private officials or buy high technology equipment to protect their operations such as electronic scanners to warn them of surveillance. Drugs are the main source of money needing laundering but most other criminal activities are generating illicit funds needing disguise. Gold Smuggling is a facet of laundering in Australia as are Casino's and the luxury goods industry. Illegal trafficking of people is also a growing problem with syndicates of Iraqis and Afghans operating route overland from the Middle East to Indonesia. From there fishing boats take the 'illegals' onto the North West coast. Outlaw Motorcycle Gangs are present in Australia, with international outlaw clubs like the Bandidos and Hells Angels and Gypsy Joker as well as locals such as the Coffin Cheaters, the Comanchero, the Nomads, the Notorious and the largest of the Rebels who have 29 chapters and are run by former boxer and founding member, Alex Vella with around 2,000 members. Youth Gangs have flourished throughout many of the large cities of Australia, especially Melbourne and Sydney, but also more recently throughout the outer suburbs of Brisbane as well. There have also been a few cases of Australian gangs imitating American street gangs such as the Bloods, including gangs such as Butch Lesbian Soldiers (BLS), Village People and FLC. New Zealand's experience of organised crime started in the 1970s. A gang, run by Terry Clark and his English followers dominated drug trafficking and other crimes, but following his imprisonment, others moved in to fill the vacuum. Today organised crime is largely carried out by motor cycle and street gangs, and criminal elements of the Asian community. The major suppliers of drugs, mainly marijuana amphetamines and LSD are the motor cycle gangs and they also are known to deal in firearms. They also have interests in massage parlours and are involved in debt collection! The Hells Angels (Auckland) was in fact the first chapter established outside California (1961). Also two other US groups, The Bandidos and the Outlaws also have interests on the Islands.

Terrorist Designations by Australia

The Australian government lists 18 organisations,²² largely Al-Qaeda and related Islamic terrorist groups including; Abu Sayyaf Group; Al-Qaeda (AQ); AQAP; AQIM; AQI; Al-Shabaab; Ansar al-Islam (formerly known as Ansar al-Sunna); Hamas' Izz al-Din al-Qassam Brigades; Hezbollah External Security Organisation; Islamic Movement of Uzbekistan (IMU); Jabhat al-Nusra; Jaish-e-Mohammed (JeM); Jamiat ul-Ansar (JuA) formerly known as Harakat Ul-Mujahideen; Jemaah Islamiyah (JI); Kurdistan Workers Party (PKK); Lashkar-e-Jhangvi (LeJ); Lashkar-e-Tayyiba (LeT); and the Palestinian Islamic Jihad (PIJ).

New Zealand

The Polynesian Maori reached New Zealand in about AD800. In 1840, their chieftains entered into a compact with Britain, the Treaty of Waitangi, in which they ceded sovereignty to Queen Victoria while retaining territorial rights. That same year, the British began the first organised colonial settlement. A series of land wars between 1843 and 1872 ended with the defeat of the native peoples. The British colony of New Zealand became an independent nation in 1907 and supported the UK militarily in both world wars.

The Asian community in New Zealand has increased dramatically in the last decade as a result of increased immigration and has unwittingly brought with it gangs such as 14K, Sun Yee On and the Wo groups. Other groups emanate from Thailand, Vietnam, Malaysia, Singapore and Japan. Their repertoire includes kidnapping, extortion, fraud, burglary, smuggling (including Humans) and money laundering. Almost all of the heroin traffic is now said to be controlled by these gangs. Proportionately the Asians are far more likely to be arrested than those of European stock. The Maoris are however at the top of the list being predominant in the Mongrel Mob, Black Power and Nomad gangs.

Recently a worrying trend has been collusion between the Mongrel Mob and Asian organised crime.

Mongrel Mob

The Mongrel Mob is a New Zealand gang, originally formed in Hawke's Bay in the 1960s and early-1970s. The gang offers a surrogate 'family' for young men, most of whom are often alienated from their family via joining. Members are from New Zealand's Maori, European or other Polynesian ethnic groups, with Maori or part Maori predominating. The gang currently operates in many cities within New Zealand; some of the best known chapters include Mongrel Mob Hastings, Mongrel Mob Porirua and Mongrel Mob Notorious. Mob members are notorious for their tattooed faces and red bandannas.

Pacific Islands

Outside of Australasia the main money laundering risks are in the Pacific islands that have developed an off-shore banking offering, including company formation, the main ones being, The Solomon Islands, Vanuatu and Nauru. For example, Vanuatu has connections in particular to Thailand, Hong Kong, UK and France. More than 100 banks are registered and companies incorporated run into the thousands. Whilst many of these establishments are used for legitimate purposes, it is often suggested that the lack of transparency and ineffective oversight make them attractive vehicles for criminals who use these corporations to establish bank accounts in other countries and then launder through these foreign banks. There is no real evidence yet of transnational criminal groups operating outside Australasia, although Guam is generally regarded as possibly the most important transshipment point for the heroin in the Pacific which moves from South East Asia to the US Drug traffickers find it useful to 'break bulk' of heroin shipments and use the US Postal System in Guam for smaller quantities

Vanuatu

Vanuatu, previously known as New Hebrides, welcomed waves of colonizers, in the millennia preceding European exploration in the 18th century. This settlement pattern accounts for the complex linguistic diversity found on the archipelago to this day. The British and French, who settled the New Hebrides in the 19th century, agreed in 1906 to an Anglo-French agreement, which administered the islands until independence in 1980, when the new name of Vanuatu was adopted.

Vanuatu is one of the few pure tax havens in the world and particularly in Asia and Oceania it hosts an established pure offshore financial centre located in the South Pacific Region. The finance centre was established in 1971 and has many classic offshore financial features, including: no exchange controls; no reporting in relation to movements of funds; confidentiality being assured, particularly for offshore entities, due to classic secrecy provisions; express establishment of International Business Companies (IBC) (within 1 hour on special request); an IBC need not lodge any other returns and need not disclose the shareholding.

Whilst many of these classic features have legitimacy, they also present opportunities and exhibit vulnerabilities which may encourage criminal enterprises and money launderers to flourish and develop. In particular allegations have been made that Vanuatu has been used aggressively for money laundering by the Russian Mafia.

Americas



The history of the Americas; North, South, and Central America, and the Caribbean, was first inhabited by people migrating to these areas from Asia during the height of the Ice Age, most likely over the then Bering land bridge across what is now Alaska.

Cultural traits brought by the first immigrants later evolved and spawned such cultures as Iroquois on North America and Pirahá of South America. These cultures later developed into civilizations, such as the Norte Chico, Cahokia, Zapotec, Toltec, Olmec, Maya, Aztec, Purepecha, Chimor, Mixtec, Moche, Mississippian, Puebloan, Totonac, Teotihuacan, Huastec people, Tarascan, Izapa, Mazatec, Muiscas, and the Inca.

Around 1000, the Vikings established a short-lived settlement in Newfoundland, but it wasn't until Spain sponsored a major exploration led by Christopher Columbus in 1492; that led to the extensive European colonisation of the Americas. The Europeans brought old world diseases which are thought to have caused catastrophic epidemics and a huge decrease of the native population. Columbus came at a time in which many technical developments in sailing techniques and communication made it possible to report his voyages easily and to spread word of them throughout western Europe. It was also a time of growing religious, imperial and economic rivalries that led to a competition for the establishment of colonies.

America got its name, according to conventional wisdom, from the great Florentine explorer, astronomer and cartographer, Amerigo Vespucci who served first the Spanish and then Portuguese monarchs as a navigator, made three trips to the shores of the land that later would be called South America, in 1499, 1501 and 1503. During these journeys he made up several maps of the new territory, but the originals have not survived. Still later mapmakers seemingly copied these original maps and included a latinised version of Amerigo, placing the name over the location for Brazil, calling it Americus and America.

Whilst the term America has stuck it was often also described as the "New World" covering 28.4% of the world's total land area and home to more than 900 million people, with the most populous countries being the US, Brazil and Mexico and the most populous cities being Mexico City, Sao Paulo and New York City.

In 1494, Spain and Portugal were the two greatest maritime European powers in the world. Anticipating that new lands would be found to the west the two nations, with the blessing and authority of the Pope in Rome, agreed the Treaty of Tordesillas which asserted that all the land outside Europe should be shared exclusively between them. In Tenochtitlan (in what is now Mexico City) on the 1st of July 1520 the Aztec Emperor Montezuma died at the hands of the Spanish invaders led by Hernan Cortes. Thus began the process of imperial expansion that was dominated first by Spain and then Portugal, from Central America throughout the Southern Continent. They would soon be joined in particular in the Caribbean by other maritime powers such as The UK, Denmark, France and the Netherlands.

The formation of sovereign states in the New World begins with the US Declaration of Independence of 1776. The American Revolutionary War lasted until 1783. The Spanish colonies won their independence in the first quarter of the 19th century, in the Spanish American wars of independence. Simón Bolívar and José de San Martín, among others, led their independence struggle. Although Bolívar attempted to keep the Spanish-speaking parts of the continent politically allied, they rapidly became independent of one another as well.

Slavery has had a significant role in the economic development the New World after the colonization of the Americas by the Europeans. The cotton, tobacco, and sugar cane harvested by slaves became important exports for the US and the Caribbean countries.

From the 1823 Monroe Doctrine onwards, the main quasi-imperial push came however from the US.

Whether exerting influence by direct military occupation; coups or economic pressure the US have always seen Central America and beyond this South America as firmly within its sphere of influence. This history informs much of what happens in Central and South America today.

Whilst imperial and colonial powers have left their impressions across the region, both in the form of culture and language, the countries in the Region have matured in most cases as independent democratic nations, though many still retain major challenges. Many countries overcoming terrorist threats but succumbing to organised criminal gangs, not only from South and Central America and in particular from the drug trafficking organisations but also to North American gangs ranging from the traditional Italian American Mafia to Street Gangs, Prison Gangs and Outlaw Motorcycle Gangs.

United States



The US achieved its independence from Britain in 1776. The Union started with 13 States and expanded during the 19th and 20th centuries, adding 37 more states. The US became the world's leading industrial power at the turn of the 20th century and by the

21st Century was the Worlds only remaining superpower, after success in two World Wars and by defeating the Soviet Union in the so cold Cold War. The US has played a major role in outlawing dangerous drugs, calling for a war on drugs, outlawing corruption, aggressively targeting organised crime and financial crime, including going after the proceeds of all crimes and since the 9/11 attack on America is the leader in the so called war on terror, utilising sanctions and co-opting anti money laundering instruments accordingly.

US foreign policy has undoubtedly had an impact, though not all positive, for example, during the Cold War, corrupt and authoritarian regimes were supported as bulwarks against communism and or Islamism, and trafficking in drugs and arms have been at least tolerated in pursuit of other interests. Also notwithstanding the US governments undoubted attempts to combat criminal activity, the US is the world's largest market for criminally generated profits with over 35% of total global criminal proceeds generated in the US. The US is the largest consumer of cocaine (shipped from Colombia and other Andean countries through Mexico and the Caribbean), as well as a major consumer of heroin, marijuana, ecstasy and methamphetamine. It is also the largest consumer of counterfeit and pirated products, and a major destination for trafficked persons, for smuggled goods, for theft and robberies. The US has the largest financial markets in the world and is vulnerable to financial frauds, to insider dealing and market manipulation. There are many infamous examples that can be found throughout Part 2 Section 7 below.

As far as terrorism is concerned, the main threat remains Al-Qaeda and its affiliates and supporters related, although these threats remain largely overseas. Terrorism financing has been largely addressed with respect to US based financing from Charities and other similar groups, in particular for Al-Qaeda but also other Arab terrorist Groups such as Hamas and Hezbollah.

US Designated Terrorist Organisations

The US lists Organisations as Foreign Terrorist Organisations²³ and also places organisations on the Terror Exclusion List.²⁴ Foreign Terrorist Organisations:

Abu Nidal Organisation; Al-Aqsa Martyrs' Brigades; Hamas; Army of Islam; Islamic Jihad Group; Palestine Liberation Front; Popular Front for the Liberation of Palestine; Popular Front for the Liberation of Palestine-General Command; Abdullah Azzam Brigades; Al-Qaeda Kurdish Battalions (formerly Ansar al-Islam); Khata'ib Hezbollah; Kurdistan Workers' Party (PKK) including KADEK and Kongra-Gel; Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn formerly Jama'a al-Tawhid wa'al-Jihad; the al-Zarqawi Network; or Al-Qaeda in Iraq or Al-Qaeda in the Land of the Two Rivers; Asbat al-Ansar; Hezbollah; Kahane Chai; Party of Free Life of Kurdistan (PJAK); Jundallah; Al-Qaeda; Al-Qaeda in the Arabian Peninsula (AQAP); Al-Qaeda in the Islamic Maghreb (formerly GSPC); Haqqani Network; Harkat-ul-Jihad al-Islami (HUJI-B); Indian Mujahideen (IM); Aum Shinrikyo; Harakat ul-Mujahideen (HUM); Jaish-e-Mohammed (JEM); Lashkar-e Tayyiba (LET); Lashkar i Hangvi; Tehrik-i-Taliban (TTP); Jemaah Anshorut Tauhid (JAT); Jemaah Islamiya; Abu Sayyaf Group (ASG); Communist Party of the Philippines/New People's Army (CPP/NPA); Islamic Movement of Uzbekistan (IMU); Islamic Jihad Union (IJU); Al-Shabaab; Gama'a al-Islamiyya; Libyan Islamic Fighting Group (LIFG); Lord's Resistance Army; Ansar Dine; Continuity Irish Republican Army (CIRA); Real Irish Republican Army (RIRA); 32 County Sovereignty Movement; Revolutionary Organisation 17 November; Revolutionary Struggle; Revolutionary People's Liberation Party/Front; Euskadi Ta Askatasuna (ETA); National Liberation Army (ELN); Revolutionary Armed Forces of Colombia (FARC); United Self-Defense Forces of Colombia; Shining Path (SL).

US Gangs

The US is also home to approximately 1.4 million active Street, Prison and Outlaw Motorcycle gang members, comprising more than 33,000 gangs, are criminally active within the US. This represents a 40% increase from an estimated 1 million gang members in 2009, with Arizona, California, and Illinois with the highest number of gang members. As Gangs are expanding, they are evolving and posing an increasing threat to US communities. Many gangs are sophisticated criminal networks with members who are violent, distribute wholesale quantities of drugs, and develop and maintain close working relationships with members and associates of transnational criminal/drug trafficking organisations. Gangs are becoming more violent while engaging in less typical and lower-

risk crime, such as prostitution and white-collar crime. Gangs are more adaptable, organised, sophisticated, and opportunistic, exploiting new and advanced technology as a means to recruit, communicate discretely, target their rivals, and perpetuate their criminal activity.

Many communities are also experiencing an increase in ethnic-based gangs such as African, Asian, Caribbean, and Eurasian gangs. Major cities and suburban areas experience the most gang-related violence. Local neighborhood-based gangs and drug crews continue to pose the most significant criminal threat in most communities. Aggressive recruitment of juveniles and immigrants, alliances and conflict between gangs, the release of incarcerated gang members from prison, advancements in technology and communication, and Mexican Drug Trafficking Organisation (DTOs) involvement in drug distribution have resulted in gang expansion and violence. Gangs are increasingly engaging in non-traditional gang-related crime, such as alien smuggling, human trafficking, and prostitution. Gangs are also engaging in white-collar crime such as counterfeiting, identity theft, and mortgage fraud, primarily due to the high profitability and much lower visibility and risk of detection and punishment than drug and weapons trafficking. US-based gangs have established strong working relationships with Central American and DTOs to perpetrate illicit cross-border activity, as well as with some organised crime groups in some regions of the US. US-based gangs and DTOs are establishing wide-reaching drug networks; assisting in the smuggling of drugs, weapons, and illegal immigrants along the Southwest Border; and serving as enforcers for DTOs interests on the US side of the border. Many gang members continue to engage in gang activity while incarcerated. Family members play pivotal roles in assisting or facilitating gang activities and recruitment during a gang members' incarceration. Gang members in some correctional facilities are adopting radical religious views while incarcerated. Gangs encourage members, associates, and relatives to obtain law enforcement, judiciary, or legal employment in order to gather information on rival gangs and law enforcement operations. Gang infiltration of the military continues to pose a significant criminal threat, as members have been identified on both domestic and international military installations. Gang members who learn advanced weaponry and combat techniques in the military are at risk of employing these skills on the street when they return to their communities. Gang members are acquiring high-powered, military-style weapons and equipment which poses a significant threat because of the potential to engage in lethal encounters with law enforcement officers and civilians. Typically firearms are acquired through illegal purchases; straw purchases via surrogates or middle-men, and thefts from individuals,

vehicles, residences and commercial establishments. Gangs are becoming increasingly adaptable and sophisticated, employing new and advanced technology to facilitate criminal activity discreetly, enhance their criminal operations, and connect with other gang members, criminal organisations, and potential recruits nationwide and even worldwide.

Gang membership continues to expand throughout communities nationwide, as gangs evolve, adapt to new threats, and form new associations. Consequently, gang-related crime and violence is increasing as gangs employ violence and intimidation to control their territory and illicit operations. Many gangs have advanced beyond their traditional role as local retail drug distributors in large cities to become more organised, adaptable, and influential in large-scale drug trafficking. Gang members are migrating from urban areas to suburban and rural communities to recruit new members, expand their drug distribution territories, form new alliances, and collaborate with rival gangs and criminal organisations for profit and influence. Local neighborhood, hybrid and female gang membership is on the rise in many communities. Prison gang members, who exert control over many street gang members, often engage in crime and violence upon their return to the community.

American Street Gangs

The most notorious American street gangs have been formed from the streets of major cities like Los Angeles, which have spawned the [Crips](#) and the [Bloods](#), [Mara Salvatrucha -13 or MS-13](#) and the [18th Street Gang](#), the [Latin Kings](#), [Wah Ching](#) and the [Black Family](#). First generation gangs are traditional street or prison gangs, essentially focussing on events within a set area, often known as their turf. Protection of their designated area and group loyalty are commonly the primary focus of first generation gangs. Their criminal activity is predominantly opportunistic and of limited sophistication. Second generation gangs are groups focussed on entrepreneurial business, commonly in the drugs trade. Their markets are expanded and maintained using violence, and competition is combated in similar fashion. These gangs sometimes have an explicit political agenda and their operations extend over a larger area than first generation gangs, even crossing national borders. Third generation gangs are organisations that have formulated very clear political goals. These groups operate trans-nationally and even globally, engaging in often large scale mercenary activity.

The Crips - US

The Crips are a primarily, but not exclusively, African-American street gang, with some members being white, Hispanic and Asian and with an estimated

membership of 30-35,000. They were founded in Los Angeles, California, in 1969 by Raymond Washington and Stanley Williams. The states with the highest estimated number of Crips sets are California, Missouri, Oklahoma and Texas. Raymond Washington and Stanley Williams were the founders of the Crips in 1969, both aged 17. The two decided to unite their local gang members from the west and east sides of South Central Los Angeles in order to battle neighboring street gangs. Washington, who attended Fremont High School, was the leader of the East Side Crips, and Williams, who attended Washington High School, led the West Side Crips. The gang's name is said to stem from the amalgamation of the word 'crib' and the acronym R.I.P (Rest In Peace); denoting both the youth of many of its members as well as the birth to death commitment they make in joining the group. The Crips gang began as a small group, later expanding into a network of sects akin to a federal body made up of independently operating sub-units. The original set came into existence after a generational divide within the Avenues Gang led to the formation of the Baby Avenues, who later became the Avenue Crips and eventually the Crips. Lack of centralised authority can however undermine the group's cohesion, allowing feuds to develop between different sects despite their common Crip affiliation. Chief among these inter-Crip rivalries is the long enduring and highly costly feud between the 83 Eight Trays and the Rolling 60s. At their outset the Crips filled a void in the community for teenage youths left by the Black Panthers following the clamp down on this group by law enforcement. In particular the first Crips sects shared a similar ideology of 'armed vanguardism' with their Panther predecessors. The gangs attraction for disillusioned youth was increased further by the downturn in social and economic conditions seen in the Los Angeles area during the 1970s. As the US government introduced a political agenda intent on large-scale disinvestment and privatisation with significant cuts to welfare, unemployment levels soared, as did dissatisfaction with government provisions. Unsurprisingly this afforded the Crips a prime environment in which to recruit members. In terms of organisation each Crip sect claims a territorial patch known as a 'hood', and the proliferation of sects across geographical boundaries comes as a result of both cultural dissemination and structural expansion. Predominantly young people adopt the characteristic traits and image of Crip members in an act of emulation, a process that commonly leads them to join an existing sect or establish their own. Film and music have proved particularly effective avenues by which the gang's sects have proliferated, with Snoop Dogg standing as the foremost example of a Crip artist commanding a global following. In this way some

aspects of Crip culture and ideology have spread almost imperceptibly to distant places and people across the world, causing sects to spring up without a direct connection to existing gangs. The Crip gang identity is therefore largely one of association with characteristic traits rather than the extension of a cohesive network. For the most part the authority within these groups is horizontal, resulting in a more egalitarian relationship between members of the same age.

The Bloods - US

This gang was founded as a predominantly African American group in Los Angeles, borne out of the conflicts between black youth groups and the [Crips](#). It was the aggressive moves towards expansion made by the [Crips](#), attempting to force many other criminal sects into submission and assimilation, which also led to the formation of an allegiance between diverse sects seeking to resist this process. The [Crip](#) opposition at the group's core is evident in the Blood's subculture, formulated according to Dwight Conquergood by a process of 'affirmation by negation' whereby almost every aspect of Blood imagery is dictated by the need to oppose the symbolism of their rivals. Among the most universal symbol employed by the group is the wearing of a red bandana in the back right pocket of their trousers. Members also walk and dance in a signature style known as Blood-walk, and tend to avoid the use of the letter C in writing, replacing it with a K or writing it backwards as a sign of disparagement towards their [Crip](#) enemies. In terms of structure the Bloods maintain a very similar organisational framework to their [Crip](#) adversaries, functioning as individual sects bound together into a single federation style entity. Groups controlling an area are commonly known as 'hoods', within which may be a number of 'sets', each controlling a certain portion of the territory. The Bloods do not possess a formal written constitution or indeed a cemented body of rules. Rather the Blood code of conduct is learnt through interaction with existing members, with new joiners learning by the example of their seniors. While there have been inter-set conflicts within the Bloods, none of these disputes have escalated into a long-term feud. The high level of cohesion within the organisation is demonstrated by the ability of members to transfer from one area to another as required. Expansion of the group has occurred as a result of smaller sects seeking protection, as well as a recruitment boom driven by the cocaine epidemic of the 1980s. Incarceration of members in prisons in other US states has afforded Bloods the opportunity to establish sets across the country, and much like the [Crips](#), cultural dissemination also played an important role in the proliferation of sets, exposing a wide audience to the gang's subculture via film and music. Despite the deeply ingrained feud underwriting the identity of the Bloods,

the history of Crip-Blood relations has not always been one of perpetual conflict. In 1992 a Gang truce was called and peace talks between the two groups followed. While these ultimately failed prominent Blood members continued an attempt to politicise their group and sought to unite the *Crips* and *Bloods* as the vanguard of the new civil rights movement.

Mara Salvatrucha -13 - US

Also known as MS-13, MS and Mara, this gang with a total membership of perhaps 6-19,000, also originated in the streets of Los Angeles amongst predominantly Salvadoran individuals. These men migrated to the US during El Salvador's civil war where, many of them were drilled in the techniques of guerrilla warfare and thoroughly accustomed to a criminal way of life. The gang was originally formed as a means of self protection against the predations of pre-existing Mexican gangs in America, and members of MS-13 were known as Maras. MS-13 now operates in more than 42 states and the District of Columbia, with 6,000-10,000 members nationwide. Members work not only in illegal enterprises, but support themselves financially through involvement with legitimate business. Such involvement in legitimate enterprise can prove a convenient method of disguising the criminal connections of MS-13 members. The reach of the group has extended beyond the US, successfully establishing sects in Canada, Mexico and Central America, controlling village communities in El Salvador, Honduras and Guatemala. MS-13 is known to be heavily involved in the drugs trade and the human trafficking industry, fighting gun battles with Mexican law enforcement in US/Mexican border areas in defence of this revenue stream. Members of the group are also associated with robbery, extortion, prostitution, and the illegal arms trade. Recently their have been unconfirmed fears that MS-13 has embarked upon relations with political terrorists. Group member or Maras are noted for their identifying tattoos, predominantly gothic in style, which cover large portions of the torso and even face. A shaven head and goatee is also a common image amongst the members of MS-13. For the most part it is an all male organisation, though women are permitted to join and a few occupy prominent roles. As with most urban gangs, the majority of membership is derived from marginalised urban areas with high unemployment levels. Areas of economic and social degradation are highly susceptible to inroads from this organised crime network. Of particular concern for law enforcement organisations is MS-13's transnational reach, evidenced most prominently in its transnational communications. Much like the *Crips*, MS-13 also boasts its own culture, one that for MS-13 is centred on the wearing of tattoos and a brutal subcultural moral code. In 2004 the FBI

deemed the risk posed by MS-13 great enough to warrant the creation of a task force singularly dedicated to combating the group; the MS-13 National Gang Task Force (NGFT). This body coordinates efforts to bring law enforcement cases against the gang.

18th Street Gang - US

Though known by a single name 18th Street Gang is in fact a collection of around 20 individual and largely autonomous sects. Formed in the late 1960s in the Rampart areas of Los Angeles, it was at first a sub-sect of the larger Clanton 14th Street neighbourhood gang. The members of 18th street gangs adhere to a strict set of rules, forbidding that they partake in drug abuse and subjecting them to strictly disciplined code of conduct. It is sometimes referred to as the Children's Army due to the recruitment of youths during their elementary and middle school stages of education. 18th Street is involved in a wide spectrum of criminal activity, however it has a heavy involvement in the production of counterfeit immigration and naturalization documents and therefore plays a significant role in both illegal immigration and human trafficking. The gang's main rivalry exists with MS-13, another organised crime network originating in Los Angeles. The gang now has a total membership tally in excess of 30,000 and extends across North America. Originally a Hispanic gang, it is now a multi-racial and multi-national gang, including African Americans, Asians, Caucasians and Native Americans. Some experts suggest that the transnational capabilities of this gang have been aided by US deportation policies, effectively transporting American gang culture to central Mexico. This allowed strong links to form between sects located in America, and those establishing themselves in Central America. As a result of its size and international character it has been claimed that 18th Street gang may have made the transition from a second generation gang into a third generation gang.

Latin Kings - US

The Almighty Latin King and Queen Nation or the Latin Kings for short, is the largest and one of the most organised Hispanic street gangs in the US and was formed in Chicago in the 1940s and consisted predominantly of Puerto Rican males. Although it was created by Puerto Ricans, most factions of the gang are now dominated by Mexicans, specifically in the Midwest, and Chicago - the city with the second largest Mexican population in the US. Originally created with the philosophy of "overcoming racial prejudice" and creating an organisation of "Kings," the Latin Kings evolved into a criminal enterprise operating throughout the US under two umbrella factions—Motherland, also known as KMC (King Manifesto and Constitution),

and Bloodline (New York City). All members of the gang refer to themselves as Latin Kings and, currently, individuals of any nationality are allowed to become members. The membership of Latin Kings is estimated to be 20,000 to 35,000 for KMC and of Bloodline as many as 7,500. The gang's primary source of income is the street-level distribution of powder cocaine, crack cocaine, heroin, and marijuana. Latin Kings continue to portray themselves as a community organisation while engaging in a wide variety of criminal activities, including assault, burglary, homicide, identity theft, and money laundering. A Latin King gang member showing his gang tattoo, a lion with a crown, and signifying the 5 point star with his hands. According to John H Richardson in the February 1997 issue of the New York Magazine, "What also made the Kings different was their unique mixture of intense discipline, revolutionary politics and a homemade religion called "Kingism"—adding idealism and a bootcamp rigor to the usual gang camaraderie—a potent mixture for troubled ghetto kids whose lives lacked structure and hope".²⁵ The Latin Kings operate under strict codes and guidelines that are conveyed in a lengthy constitution, and they follow the teachings of the King Manifesto. According to the Latin King Manifesto, there are three stages or cycles of Nation life that constitute Kingism. They are: The Primitive Stage: wherein the neophyte member is expected to be immature and to be involved in such activities as gang-banging and being a street warrior without the full consciousness of Kingism. The Conservative Stage: which is where a member tires of the street gang life but is still accepting of life as it has been taught to him by the existing system that exploits all people of color, dehumanizes them, and maintains them under the conditions and social yoke of slavery. The New King Stage: where the member "learns that his ills lie at the roots of a system completely alien to his train of thought and his natural development, due to the components of dehumanization that exist therein". According to the Manifesto, "The New King is the end product of complete awareness, perceiving three-hundred and sixty degrees of enlightenment; his observations are free and independent; his thoughts are not clouded by any form of prejudice...For him there are no horizons between races, sexes and senseless labels", including gang labels for recognition. The New King no longer views the rival warrior as the cause of his ills; instead, he fights against the Anti-King System (social injustices and inequality), a system which seeks to deny and oppress his people: the Oppressed Third World Peoples.

Wah Ching - US

Wah Ching also known by slang as "Dub C" is a Chinese street gang that originated in San Francisco's Chinatown in the 1960s. The name literally translates to "Chinese youth," and the group was comprised primarily of immigrant Cantonese boys from Hong Kong who banded together to combat the American-born Chinese who would often pick on them. From its origin in 1966 as a street gang, the Wah Ching has developed into a criminal organisation, with alleged multi-international crime connections. During the 1970s and 1980s, the Wah Ching became an organisation that controlled most of the criminal vices in San Francisco's Chinatown and Los Angeles' Chinese communities. During that time, there may have been as many as 200 Wah Ching members and 500 criminal associates in California. Although primarily headquartered in San Francisco, they have developed strong associations with Asian organised crime groups and gang members in Los Angeles, Seattle, Vancouver, Toronto, Boston, and New York—along with close ties to the Sun Yee On and the 14K Triad in Hong Kong. Today in Los Angeles, The Bay Area California, Vancouver, and the rest of the West Coast of North America there is an estimated 3,000 gang members of Wah Ching and an estimated 1,000 more affiliated with the Wah Ching Gang. Wah Ching first received widespread media attention because of the 1977 Golden Dragon massacre involving another Chinese gang, the Chung Ching Yee (Joe Boys). The event took place at the Golden Dragon Restaurant in San Francisco's Chinatown. The cause of the attack was vandalism by Wah Ching to the graves of several Joe Boy members and a shootout that took place a few months earlier that left one Joe Boy dead and two others wounded. In the 1990s, a Hong Kong Triad called Wo Hop To set foot in San Francisco to take over all Asian Organised Crime in America. At that time Wah Ching and Wo Hop To became partners in crime activities. But later, turned into rivals after one of the Wah Ching leaders was gunned down at Purple Onion Restaurant in North Beach by members of the Wo Hop To, and that triggered a war. Soon, bullets were flying in the streets of Chinatown. More and more Wah Chings were being murdered and Wah Ching was ran out of San Francisco ever since. Wah Ching is located in the Northern California Bay Area and in Southern California. Their main enemies are the Asian Boyz (ABZ) and Vietnamese Boyz (VBZ). Both Wah Ching and Asian Boyz were featured on the television programme, America's Most Wanted, following a vicious shooting at a pool hall. Wah Ching's move from its original home in the Bay Area to the southern California region is a sources of dispute over gang turf. Currently, the gang have shown signs of mixed ideology. Despite the fact that Wah Ching in Chinese literally means "Chinese Youth," there are still some individuals of non-Chinese descent who claim Wah Ching. The gang now consists of a great

number of Vietnamese members, and the same with their rivals, the Vietnamese Boyz holds a great number of Chinese members. It is rumored that their reasoning for this is that it is the "Chinese Youth" gang, and that the members working or fighting for the gang do not have to be of Chinese ethnicity.

Black Guerrilla Family (Black Family, Black Vanguard) - US

Founded in 1966 by George Jackson, located in Marin County, California, the Black Guerrilla family was established in order to maintain Black dignity in prison as well as planning the overthrow of the US government. Standing as one of the most politically influenced gangs, the Black Guerrilla Family has very strong emotions towards Marxism. Today, the Black Family has about 50,000 gang members, many of which who are associated with other gangs. In order to join the gang, one must be black, and must be nominated by an already existing member. Recently it has been said that the gang is experiencing internal conflicts between old and new members

American Prison Gangs - US

Prison gangs are criminal organisations that originated within the penal system and operate within correctional facilities. With over 20 million incarcerated in the US it is no surprise that Prison Gangs are at their most endemic and organised here. Whilst the Gangs originate from the Prison system, released members operate also on the street and so compete with Street Gangs. The main Prison Gangs in the US are the Aryan Brotherhood, Mexican Mafia, La Nuestra Familia and the Texas Syndicate.

The Aryan Brotherhood - US

A white supremacist prison gang and crime syndicate, specialising in drug trafficking, extortion, inmate prostitution and commercial assassination with more than 20,000 members. The organisation was established in 1964 by a group of Irish Bikers directly opposing a militant black group known as the Black Guerrilla Family within San Quentin state prison. This feud has led to their allegiance with the Mexican prison gang Mexican Mafia (La eMe), a bond forged from mutual animosity towards the Black Guerrilla Family. As a result of their racially orientated initial aims the group was dismissed for a time as merely a marginal white supremacist movement. However since then the Aryan Brotherhood has grown to control prisons in California, Illinois, Texas, and Kansas. Despite operating from within prison, the reach of the Aryan Brotherhood extends far beyond their cell walls with released gang members maintaining communications between disparate prisons and exacting the commands of their

predominantly confined leaders. The ability of the Aryan Brotherhood to operate in this manner raises the question of how a criminal organisation already serving punishment sentences in secure facilities can possibly be combated further by law enforcement. A glimmer of hope was offered by the organisation's hierarchical structure, leading prosecutors in 2002 to seek death sentences for the group's most prominent members. By literally striking at the root of the Aryan Brotherhood they hoped to render this seemingly irrepressible group dysfunctional, embarking on the largest death penalty case in US history. It was however an endeavour that ultimately ended in failure, without a single case achieving the sought after death sentence. As a result the organisation's ruling echelon endured and the gang continued to proliferate. Other law enforcement attempts to reduce the influence of the group have met similarly unsuccessful ends, with state authorities separating members by moving them to other prisons. This approach served only to transplant shoots of the Aryan Brotherhood's network, with new sects forming in the other prisons to which group members were rather naively 'exiled'. The extent of the influence exerted by the Aryan Brotherhood within the US penal system is aptly demonstrated by the FBI's calculation that despite the gang constituting less than 1% of the total inmate population, they were nevertheless responsible for almost 18% of prison murders in 2005.²⁶

Mexican Mafia (La eMe) - US

The Mexican Mafia is a gang that has its strongholds in many prisons throughout the US. The gang was started in the 1950s in Tracy California. La eMe is well known for its drug trafficking, extortion, and murder. Closely knit with the Aryan Brotherhood, La eMe has made many contracts with ally gangs in order to kill other rival gang members. The gang doesn't have many rules for its members: no exposing the gang, no homosexual acts, and no cowardice. Mexican Mafia gang members also cannot practice the Christian religion. Once you join the Mexican Mafia and are released from jail, members are expected to send some of their earnings to those lead gang members who are still in jail. The gang isn't known to kill random civilians.

La Nuestra Familia - US

La Nuestra Familia is a Mexican American prison gang that originated in Northern California. The gang has been around since 1968 and has always been a rival of the Mexican Mafia. Many speculate that the gang was created just to deliver a blow to their rival gang. The gang puts a high focus on protecting as well as preserving the Chicano culture, especially while living in a society that is dominated by so many different races. La Nuestra Familia is known to control intra-

prison drug and sex trades. From the prison, high-up gang members call to those outside of the prison directing operations. The gang is known to kill anyone, sometimes members of the gang. Members of La Nuestra Familia are known to be serious criminals and the gang requires a two year time period to join. La Nuestra Familia requires that all gang members put the gang above family, money, drugs, and women. Women cannot join the gang but are sometimes used for running drugs.

Texas Syndicate (Texas 7) - US

Texas Syndicate is a State Prison gang created in response to other gangs like the Mexican Mafia (La eMe) and the Aryan Brotherhood. As the gangs were preying on inmates, especially in Texas, prisoners saw a need to have a rival gang to protect the Texas prisoners as a means of self-protection. The Texas 7 doesn't allow any members that are outside of the Hispanic race. Caucasian members are extremely frowned upon. The gang is made up generally of Mexican immigrant prisoners, not Mexicans who were born and raised in the US. In 2000, the gang was said to have about 1,000 members in jail, and about 830 outside of jail. Texas Syndicate is known for contract murder, gambling, prostitution, extortion, and drug trafficking. Many of the gang's leaders are imprisoned due to drug charges.

Ku Klux Klan - US

The first KKK was founded in 1865 as a charitable organisation to help widows and orphans in the American South at the end of the civil war, when the victorious Union government imposed a version of martial law on the south and began to enforce laws designed to end segregation. When a constitutional amendment granted black men the right to vote in 1870, the group turned to intimidation and violence to try to halt de-segregation and was dismantled in 1871 by law. A second organisation by the same name was founded in 1915 and yet a third incarnation surfaced during World War II. The KKK is a white supremacist group. It holds that only white, heterosexual Christians deserve civil rights. Its mandate, to reverse the equality granted African-Americans after the Civil War expanded as the social demographics of the US changed. It also opposes civil rights for Jews, gays, Catholics, and other ethnic and religious groups. Today, the various local groups that make up the Klan often focus their hatred on immigrants. Probably their most infamous attack was carried out in 1963 with the bombing of the 16th Street Baptist Church in Birmingham, Alabama. Four girls were killed in the bombing. The bombing helped prompt President Johnson to sign the Civil Rights Act of 1964. The Klan is organised as a brotherhood, and has state and national organisation. Some believe

it has as many as 8,000 members today in about 150 Klan chapters, although estimates range from around 2,500-6,000 possible members. They used a variety of tactics to harass and intimidate blacks and sympathetic whites including putting burning crosses on the lawns of individuals, arson, riding in groups by horseback near communities they wanted to frighten, and beating, rape and lynching (hanging). The KKK is distinguished by its unusual costume of long robes and tall, pointy white hats. These were adopted by the first KKK and meant to represent Klansmen as ghosts of angry Confederates. These costumes are still worn today and serve as an intimidating symbol that recalls the violent history of the organisation

Weathermen-Weather Underground - US

The "Weathermen" and later the "Weather Underground," was a splinter organisation founded in 1968 from the Students for a Democratic Society, during a tumultuous time in American and world history. The Students for a Democratic Society was the most prominent symbol was founded in 1960 in Ann Arbor, Michigan, and had a broad platform of goals related to their critiques of American military interventions overseas and their charges of racism and inequality in the US. To many it appeared that national liberation movements and left-leaning revolutionary or guerrilla movements were the future in order to change the world from one that seem still to prevail from the 1950s. The name comes from a song by singer Bob Dylan, "Subterranean Homesick Blues," which contains the line: "You don't need a weather man to know which way the wind blows." The Weather Underground came out of this ethos, but added a militant spin, believing that violent action was required to effect change. Other student groups, in other parts of the world, felt the same in the late 1960s. According to the group's 1970 "Declaration of War" against the US, its goal was to "lead white kids into armed revolution." In the view of the group, "revolutionary violence" was necessary to combat what they perceived as a "war" against African-Americans, and military actions overseas, such as the Vietnam war and the invasion of Cambodia. The group was responsible for a number of attacks, including 1969 "Days of Rage" riot staged by the Weathermen in Chicago, to protest the Vietnam war; the 1971 bombing of the US Capitol and the 1972 bombing of the Pentagon.

Special Focus 13 American Mafia - US



Whilst engaging in a broad range of illegal activities, such as drug trafficking, extortion, smuggling and human trafficking, the Italian American Mafia also get involved in a range of legal business activities, for example setting up industries such as garbage

collection and waste management, construction and cement pouring, supplying Labour and operating Cash intensive business, for example restaurants. There are estimated at over 3,000 members, based largely in NYC, New Jersey, Philadelphia, New England, Detroit and Chicago as well as Montreal in Canada.

The Italian American Mafia evolved into organised criminal gangs at the start of the Twentieth Century emerging as a result of the emigration from Italy of Sicilian Mafia members, known as La Cosa Nostra in the late Nineteenth Century and home grown gangs. In 1900 in New York, Black Hand Gang came to prominence to be succeeded in the 1910s and '20s by the Five Points Gang and in the 1920s in Chicago by Al Capone's Syndicate. "Al" Capone born in New York but plying his trade in Chicago during the Prohibition era in the 1920s was dedicated to smuggling alcohol and was involved in other illegal activities such as prostitution and the bribery of government officials. Despite his illegitimate occupation, Capone became a highly visible public figure. He made various charitable donations using the money he made from his activities, and was viewed by some to be a "modern-day Robin Hood", though was dubbed by the press Americas Public Enemy No 1. Capone was publicly criticised for his involvement in the Saint Valentine's Day Massacre, when seven rival gang members were executed. Capone was eventually convicted on federal charges of tax evasion, and sentenced to federal prison. His incarceration included a term at the new Alcatraz federal prison. He died in 1947.

Despite the governments best attempts to arrest and convict Al Capone for Prohibition violations, by Bureau of Prohibition agent Eliot Ness it was IRS agent Frank J. Wilson who would bring down Al Capone building a case against Capone for income tax violations, which the government decided was more likely material for a

conviction. Frank Wilson, would later become Chief of the US Secret Service between 1937 and 1946. In 1931 Capone was indicted for income tax evasion and various violations of the Volstead Act (Prohibition). Following a long trial, he was found guilty on some income tax evasion counts (the Volstead Act violations were dropped). The judge gave him an 11-year sentence along with heavy fines, and liens were filed against his various properties. His incarceration and the repeal of Prohibition in December 1933, which reduced a major source of revenue, diminished his power.

The key to the case was provided by Edward O'Hare, aka "Easy Eddie" who was a lawyer in Chicago, and working with Al Capone he made fortune. Eddie was the father of Medal of Honor Butch O'Hare, for whom Chicago's O'Hare Airport is now named. For his part in the conviction of Capone Eddie was eventually assassinated in 1939. Frank Wilson would say that, "On the inside of the gang I had one of the best undercover men I have ever known: Eddie O'Hare." By 1930, Eddie was working undercover for the IRS. It is believed Eddie directed investigator Wilson to the Capone bookkeeper who became a key witness at the 1931 trial, and he also helped break the code with which Capone's bookkeepers kept ledgers at various gambling houses throughout the 1920s. During the Capone trial, Eddie tipped the government that Capone had fixed the original jury that was to hear the case and thus alerted, the Judge switched juries with another federal judge just as the Capone tax trial was set to begin. By the end of the 1920s two primary gangs had emerged, leading to a war for control of organised crime in New York City. The murder of gang leader Joseph Masseria brought the war to an abrupt end, the two groups uniting to form America's "La Cosa Nostra". Within six months their leader was dead, but not before establishing La Cosa Nostra's code of conduct, setting up the "family" divisions and structure, and established procedures for resolving disputes. The new leader Charles "Lucky" Luciano became the new leader, set up a "Commission" to rule all La Cosa Nostra activities. The Commission included bosses from the main crime families. Luciano was deported back to Italy in 1946 based on his conviction for operating a prostitution ring. There, he became a liaison between the Sicilian Mafia and La Cosa Nostra.

One of the families that sat on the Commission was the Genovese family for whom one of the more colorful and celebrated Mafia figures worked, Benjamin "Bugsy" Siegel who was behind the large-scale development of metropolitan Las Vegas.

Siegel was born in 1906 in Brooklyn, New York City. Newspapers would refer to him as "Bugsy", (said to

be based on the slang "bugs", meaning "crazy", and used to describe his erratic behavior). In 1934, Siegel had traveled to Nevada searching for opportunities to provide illicit services to the men constructing the Hoover Dam. Whilst Siegel had been given control over the Nevada desert, he failed to exploit it. Its potential was well known, for example, Al Capone had earlier, eyed the empty desert in the mid-'30s, but never forged ahead with his plans of turning it into a hotel and gambling haven. In 1937, Mafia bosses sent Siegel to California to develop gambling ties with Los Angeles mobsters, where he enjoyed a Playboy lifestyle living in Beverly Hills. Bugsy would end up returning to the desert after the end of World War 2 first organizing labour and materials for the construction of a hotel in the middle of nowhere. The Hotel, the Flamingo would soon be owned and controlled by Bugsy for the Mafia and would be the very first Hotel Casino built on the now famous strip in Las Vegas. Bugsy never saw the success that would ultimately flow from the development of Las Vegas, with the Flamingo being built lavishly, massive cost overruns angered his bosses and Bugsy was killed soon after the opening.

With the repeal of Prohibition in 1933, the Mafia moved beyond bootlegging and into a range of underworld activities, from illegal gambling to loan-sharking to prostitution rings. The Mafia also involved itself in labour unions and legitimate businesses, including construction, garbage collection, trucking, restaurants and nightclubs and the New York garment industry, and raked in enormous profits through kickbacks and protection shakedowns. Instrumental to the Mafia's success was its ability to bribe corrupt public officials and business leaders, along with witnesses and juries in court cases.

In 1970, Congress passed the Racketeer Influenced and Corrupt Organisations (RICO) Act, which proved to be a powerful tool in the government's war on the Mafia, as it allowed prosecutors to go after crime families and their sources of revenue, both legal and illegal. During the 1980s and 1990s, RICO laws were used to convict numerous high-level mobsters. Some Mafiosi, faced with long prison sentences, broke the once-sacred code of omerta and testified against their fellow mobsters in exchange for a place in the federal witness-protection programme. By the start of the 21st century, the American Mafia was a shadow of its former self. However, the Mafia remained active in some of its traditional ventures, including loan-sharking and illegal gambling, and its involvement in labour unions and legitimate industries such as construction hasn't been completely eliminated.

Contributing to the Mafia's continued survival may be the fact that following the 11 September 2001, terrorist attacks on America, significant resources devoted to investigating organised crime (which had already seen cuts prior to 9/11) were shifted to counterterrorism work.

The Mafia's criminal activities are international with members and affiliates in Canada, South America, Australia, and parts of Europe. They are also known to collaborate with other international organised crime groups from all over the world, especially in drug trafficking. The major threats to American society posed by these groups are drug trafficking and money laundering. They have been involved in heroin trafficking for decades. Two major investigations that targeted the Italian American Mafia are known as the "French Connection" and the "Pizza Connection" See Part 2, Section 7, Criminal Cases for details.

The Mafia is still most active in New York City, but also New Jersey, Philadelphia, New England, Detroit, and Chicago. Among the five families of New York the current acting bosses include Vincent Badalamenti (Bonanno), Domenico Cefalu (Gambino), Carmine Persico (Colombo), Steven Crea (Lucchese), and Daniel Leo (Genovese). Outside of New York, the Rizzuto clan based in Montreal, Canada and led by Vito Rizzuto are often described as the Sixth Family. Beyond these, the Chicago Outfit is also important and is one of the largest crime syndicate in the US, being influenced by none other than Al Capone. One of the Chicago Outfit's biggest competitors is the Russian Mafia. Unlike most organised crime groups, the Outfit has members from other ethnicities besides Italian Americans. The leader is John "No Nose" DiFronzo.

The five families considered as the original Italian American Mafia crime families of New York City who dominated organised crime and known as La Cosa Nostra in the US since the 1930s are the Lucchese, Bonanno, Gambino, Genovese and Colombo. La Cosa Nostra with its deep ties to the Sicilian Mafia were not the only Italian Organised groups that became active in the US The Camorra or Neapolitan Mafia; the 'Ndrangheta or Calabrian Mafia; and the Sacra Corona Unita or United Sacred Crown from Puglia operate and together with La Cosa Nostra, the four groups have approximately 3,000 members in the US and more than 25,000 worldwide with perhaps 250,000 affiliates. It is believed that nearly 200 Camorra affiliates operate in the US and perhaps around the same number for the 'Ndrangheta or Calabrian Mafia. Very few Sacra Corona Unita members have been identified in the US.

Special Focus 14 Outlaw Motorcycle Gangs - US



Whilst the Hell's Angels are the best known of all the so called "Outlaw Motorcycle Gangs", the Outlaws, the Bandidos and the Pagans, make up the top 4 biker gangs with other gangs the Mongols, the Vagos Motorcycle Club and the Wheels of Soul, each of which stake

claim to territory in North America, and in Europe, particularly in the UK, Scandinavia and elsewhere, even in Australia. Membership is as high as 44,000 in the US with approximately 3,000 gangs or sub gangs in total.

An outlaw motorcycle gang (OMG) is a motorcycle subculture which has its roots in the post-World War II era of American society. It is generally centred around the use of cruiser motorcycles, particularly Harley-Davidsons and choppers, and a set of ideals which celebrate freedom, nonconformity to mainstream culture and loyalty to the biker group. In the US, such clubs were first considered "outlaw" as they are not sanctioned by the American Motorcyclist Association (AMA) and do not adhere to the AMA's rules. Instead the clubs have their own set of bylaws from which the values of the outlaw biker culture arise.

Some outlaw motorcycle clubs consider themselves "one percenters" and they wear a 1% patch on the jackets together with their main patches which designate the gang name, the gang logo and the territory claimed. The one percenter patch of honour is claimed to be a reference to a comment made by the American Motorcyclist Association (AMA) in which they stated that 99% of motorcyclists were law-abiding citizens, implying that the last one percent were outlaws. Numerous law enforcement agencies, in the USA, Canada, the UK and Australia consider OMGs to have significant involvement in both legal and criminal activity. Whilst OMG members may have legitimate jobs, and some of their activities within the Club are legitimate, such as Selling Bykes , Running Byke Events, and providing Security as well raising funds for Charities through Byke Run Events for example which provides positive PR for the OMGs there is ample evidence that the leadership of these organisations if not

all of their members do engage in systematic criminal activity. The FBI asserts that OMGs support themselves primarily through drug dealing, trafficking in stolen goods, and extortion, and that they fight over territory and the illegal drug trade and collect US\$1bio in illegal income annually. Law Enforcement see these groups as unique amongst those engaged regularly in criminality, because they maintain websites, identify themselves through patches and tattoos, have written constitutions and bylaws, trademark their club names and logos, even carry out publicity campaigns aimed at cleaning up their public image.

The US Department of Justice defines the term "Outlaw Motorcycle Gang" (OMG) as an organisation whose members use their motorcycle clubs as "conduits for criminal enterprises".²⁷ Both the US and Canada have designated four MCs as "Outlaw Motorcycle Gangs", the Hells Angels, the Pagans, the Outlaws, and the Bandidos, known as the "Big Four". The California Attorney General also lists the Mongols and the Vagos Motorcycle Club as outlaw motorcycle gangs.

Amongst the Big Four as well as between these and other small Outlaw Motorcycle Gangs there has been a great deal of rivalry with each willing to fight over territory and other issues. At times the level of violence was vicious and included murders to settle a score, retaliate against an attack or to try to intimidate another gang. There was a long running war between, for example, the Hells Angels and the Outlaws in the US for many years which led to fatal casualties on both sides. Today the level of violence is down as cooler heads seemed to have prevailed and most likely working agreements regarding territory have been established and are respected.

Perhaps the greatest violence was in Canada over the past two decades where the Quebec Biker war, involved more than 150 murders, 84 bombings, and 130 cases of arson. The increased violence in Canada was the result of turf wars over control of the illegal drug business also involving the Hell's Angels.

Whilst Law Enforcements view appears to be clear, Members and supporters of these clubs insist that illegal activities may occur but the Club is not responsible for individuals activities and that these are in fact isolated occurrences and that they, as a whole, are not criminal organisations. Contrary to other criminal organisations, OMGs operate differently to for example criminal organisations, operating on an individual basis instead of top-down, which is how supporters can claim that only some members are committing crimes. Belonging guarantees to each member the option

of running criminal activity, using other members as support - the main characteristic of OMGs being "amoral individualism" in contrast to the hierarchical orders and bonds of "amoral familism" of other criminal organisations such as the Mafia.

ATF agent William Queen, who infiltrated the Mongols, wrote that what makes a group like them different from the Mafia is that crime and violence are not used as expedients in pursuit of profit, but that the priorities are reversed. Mayhem and lawlessness are inherent in living "The Life" and the money they obtain by illegal means is only wanted as a way to perpetuate that lifestyle.

Hell's Angels - US

The Hells Angels Motorcycle Club (HAMC) is a worldwide motorcycle gang whose members typically ride Harley-Davidson motorcycles. In the US and Canada, the Hells Angels are incorporated as the Hells Angels Motorcycle Corporation. Their primary motto is "When we do right, nobody remembers. When we do wrong, nobody forgets". Members of the organisation have continuously asserted that they are only a group of motorcycle enthusiasts who have joined to ride motorcycles together, to organise social events such as group road trips, fundraisers, parties and motorcycle rallies. The Hells Angels were originally formed in 1948 in Fontana, California through an amalgamation of former members from different motorcycle clubs such as The Pissed Off Bastards of Bloomington. The name "Hells Angels" was believed to have been inspired by the common historical use, in both World War I and World War II, to name squadrons or other fighting groups by a fierce, death defying name. The Flying Tigers (American Volunteer Group) in Burma and China fielded three squadrons of P-40s; the Third Squadron was named "Hell's Angels". The 1930 Howard Hughes film Hell's Angels displayed extraordinary and dangerous feats of aviation and it is believed that the World War II groups who used that name based it on the film. The Hells Angels official website attributes the official "death's head" insignia design to Frank Sadilek, past president of the San Francisco Chapter.

The colour and shape of the early style jacket emblem (prior to 1953) were copied from the insignias of the 85th Fighter Squadron and the 552nd Medium Bomber Squadron. The Hells Angels utilise a system of patches, similar to military medals. Although the specific meaning of each patch is not publicly known, the patches identify specific or significant actions or beliefs of each biker. The official colours of the Hells Angels are red lettering displayed on a white background - hence the clubs nickname "The Red and White". These

patches are worn on leather or denim jackets and vests. Red and white are also used to display the number 81 on many patches as in "Support 81, Route 81". The 8 and 1 stand for the respective positions in the alphabet of H and A. These are used by friends and supporters of the club as only full members can wear any Hells Angels imagery.

The full requirements to become a Hells Angel are the following: candidates must be male, have a valid driver's licence, have a working motorcycle and cannot be a child molester or have applied to become a police officer or prison guard. After a lengthy, phased process, a prospective member is first deemed to be a "Hang-around", indicating that the individual is invited to some club events or to meet club members at known gathering places. If the Hang-around is interested, he may be asked to become an 'Associate', a status that usually lasts a year or two. At the end of that stage, he is reclassified as 'Prospect', participating in some club activities, but not having voting privileges, while he is evaluated for suitability as a full member. The last phase, and highest membership status is 'Full Membership' or 'Full-Patch'. The term Full-Patch refers to the complete four-piece crest, including the 'Death Head' logo, two rockers (top rocker: Hells Angels; bottom rocker: State or Territory claimed) and the rectangular 'MC' patch below the wing of the Death's Head.

Prospects are allowed to wear only a bottom rocker with the State or Territory name along with the rectangular 'MC' patch. To become a full member, the Prospect must be voted on by the rest of the full club members. Prior to votes being cast, a Prospect usually travels to every chapter in the sponsoring chapter's geographic jurisdiction (state/province/territory) and introduces himself to every Full-Patch. This process allows each voting member to become familiar with the subject and ask questions of concern before the vote. Successful admission usually requires more than a simple majority, and some clubs may reject a Prospect for a single dissenting vote. Formal induction follows, where the Prospect affirms his loyalty to the club and its members. The final logo patch (Hells Angels rocker) is awarded at this initiation ceremony. The step of attaining full membership can be referred to as "being patched". Even after a member is patched-in, the patches themselves remain the property of HAMC rather than the member. On leaving the Hells Angels, or being ejected, they must be returned to the club. The HAMC acknowledges more than one hundred chapters spread over 29 countries. The first official chapter outside of the US was formed in New Zealand in 1961. Europe did not become home to the Hells Angels until 1969. To compensate, the group purchased military surplus

motorcycles and shared weekends riding the roads and venting their frustrations about suburbia by partying hard. This is how the gang, The Hell's Angles came to stand for individualism and rebellion against authority.

The Bandidos - US

The club was formed in 1966 in Texas by Donald Chambers, an ex Vietnam Vet and Marine he modeled the clubs colors after the crimson and gold motif of the US Marine Corps and using an obese machete- and pistol-wielding Mexican Bandido as the centre patch for the club's colors. The Bandidos, also called the "Bandido Nation", is the fastest-growing outlaw motorcycle club in the world with over 90 chapters in the US, 90 chapters in Europe, and another 17 in Australia and Southeast Asia. In the US, the club is concentrated in Texas, and other parts of the South, north West and Rocky Mountain areas. In recent years the club has also expanded heavily into Northern Europe and Scandinavia in particular. Additionally, it is looking into setting up clubs in Russia and Eastern Europe and also in Singapore, Malaysia and Thailand. The Bandidos also have a large number of "support clubs." These groups usually wear reverse colors (gold border with red background rather than the Bandidos' red-border-and-gold background). They also commonly wear a "support patch" consisting of a round patch in Bandidos colors on the front upper left of the colors (vest), as worn by the member. Most of these clubs are regional.

The Outlaws - US

The McCook Outlaws Motorcycle Club was established in Matilda's Bar on old Route 66 in McCook, Illinois, near Chicago, making the Outlaws the oldest of the OMGs. Following the second World War, with new members coming from all over the Chicago area, the Club moved out of McCook re-establishing itself in Chicago, and changing its name to the "Chicago Outlaws". The club logo also underwent a change; a small skull replaced the winged motorcycle and old English style letters. The design was embroidered on black shirts and hand painted on leather jackets. A set of Crossed Pistons were added to the small skull, aping those on the jacket of Marlon Brando in the movie, "the Wild One" released in 1953 about a fictional Biker in a fictional Black Rebel Motorcycle Club. In the 1960s the Outlaws grew and new clubs also joined with in addition to Chicago, Outlaw clubs being established in New York, Kentucky and Milwaukee formed the start of the "Outlaw Nation." On January 1, 1965, the American Outlaws Association (A.O.A.) was founded. The insignia of the club, a skull and crossed pistons, is named "Charlie". In July 1967, the Outlaws National President and a number of other members travelled south from Chicago and sanctioned the club's first

chapter in Florida. "God Forgives Outlaws Don't" ("G.F.O.D.") became the club's motto in 1969.

The Pagans - US

The Pagan's Motorcycle Club, or simply The Pagans, was formed by Lou Dobkin in 1959 in Maryland. The club rapidly expanded and by 1965, the Pagans, originally clad in blue denim jackets and riding Triumphs, began to evolve along the lines of the stereotypical one percenter motorcycle club. Originally they were a comradeship of 13 motorcyclists. In the 1960s they adopted a formal constitution and formed a governing structure choosing a national president. They were a fairly non-violent group until 1965, when the Pagans evolved into a true outlaw biker gang with ties to other organised crime groups such as the American Mafia. The Pagans MC patch depicts the Norse fire-giant Surtr sitting on the sun, wielding a sword, plus the word Pagan's in red, white and blue. They can be identified by the black number 13 emblazoned on the back of their leather jackets. The Pagans boast about 350-400 members in chapters mostly on the East Coast between New York and Miami, including in New Jersey, Pennsylvania, Delaware, Maryland, West Virginia, Kentucky, Ohio, Virginia, North Carolina and South Carolina. The Pagans headquarters is currently in Delaware County, Pennsylvania. They rank as one of the fiercest outlaw biker gangs in the US.

The Mongols - US

The Mongols formed by Hispanic Vietnam vets who were denied membership to the Hells Angels, is headquartered in southern California but has a presence in 14 states and runs international chapters in Australia, Germany, Italy, Mexico and parts of Scandinavia. Allies are the Bandidos, Outlaws and the Sons of Silence.

The Vagos Motorcycle Club - US

Originally known as "The Psychos", the Vagos Motorcycle Club is active throughout southern California. Vagos, many military trained, are notoriously ruthless with their enemies and have declared war on law enforcement. They are rivals of the Hells Angels. The gang is known for producing and selling drugs, backed by violence, extortion, thievery and money laundering. They have also been accused of witness intimidation and insurance fraud.

Wheels of Soul - US

The Wheels of Soul is a predominantly black, national biker gang headquartered in Philadelphia. It is believed that the group is criminally active in at least six other states. It is believed that the Wheels of Soul also orchestrates robberies and kidnappings and is involved in the production and sale of drugs.

Canada



A North American country consisting of ten provinces and three territories Canada sits north of the continental US. It, as its motto says, extends "from Sea to Sea" i.e. Atlantic to Pacific. The world's second largest country by area it has a population of nearly 34 million. With the 11th largest economy it is one of the world's wealthiest nations.

Canadian organised crime is often remembered for its role in the US prohibition era of the early Twentieth Century. Of all the alcohol that was consumed in the US during Prohibition, 75% was smuggled across the Detroit River separating Windsor and Detroit. An estimated 25% of Windsor's citizens were involved in smuggling and during the 1920s many made fortunes. Windsor residents took every advantage and many became millionaires, building some of the most prestigious mansions in Windsor. Needless to say the sheer logistics, infrastructure and equipment of 'bootlegging' led to wholesale corruption of public officials. The repeal of prohibition in the US eventually brought a return to 'normalcy'.

In 2012, the Canadian Parliamentary Standing Committee on Justice and Human Rights produced a report entitled "The State of Organised Crime". The Report observed that 'gangs and organised crime have been with us for at least 150 years. Alienated and disenfranchised young men long ago forged a common bond of lawlessness, using crime as a means of generating wealth.'

Today the extent of organised crime in Canada is affected by many factors, not least the nearly 4000 miles border with the US (not including the 1500 miles of border with Alaska) and within its borders, an extraordinarily diverse population. It has an aboriginal population as well as the product of successive generations of immigration from all corners of the globe over the past since the 16th Century. Initially French then British immigration widened to include the rest of Europe but by 2006 Canada received nearly 237,000 immigrants from all over the world. The top 5 sending countries (in order) were China; India; Philippines; Pakistan and the US.

In 2008, over 900 organised crime groups were identified in Canada, including approximately 300 street gangs. In 2011, Criminal Intelligence Service Canada (CISC) identified 729 crime groups and categorised organised Canadian crime groups into four threat levels. Category one groups are the most significant level of threat and are those who operate between provinces or internationally. Twenty-four criminal organisations are currently in this group. Category two groups operate the same as Category one groups, but have been deemed to be at a lower threat level. There are 262 category two groups in Canada today. Category three groups are those who operate within a single province, but they can cover more than one city or region. There are 120 Category three groups operating in Canada. Finally, category four groups are confined to a single area, such as a town or a city and 210 criminal organisations belong to this category.

In 2010, of the 56 gang-related homicides committed in Canada's ten largest cities, 82% were committed in Toronto, Montréal, and Vancouver a figure one might expect, as organised crime is predominantly located in urban areas. It does however occur however in less densely populated areas such as the Prairie cities and First Nation areas.

In 2009 a Situation Report breakdown for organised crime in Quebec fell into the following categories: Asian-origin organised crime; Aboriginal-origin organised crime; Italian-origin traditional organised crime; Quebec-origin traditional organised crime; street gangs; Latin-American-origin organised crime; East European-origin organised crime; Near- and Middle-East-origin organised crime; and criminal bikers. This again reflects the makeup of various immigrant groups although some, increasingly, are becoming more heterogeneous and willing to cooperate with other groups.

Mafia groups have been in Canada since the prohibition era and often had cross border links with US Groups. In Quebec the Rizzuto crime family is the main group whilst in Ontario the Ndrangheta operates under the auspices of the Siderno Group and the Musitano family both originating from Calabria. The Rizzutto were once part of the Corleone group who in turn were regarded by the FBI as "part of" the Bonanno family in the US. Some called the Sixth Family in reference to the Five families of New York.

Other Canadian crime group types include Street gangs, Motorcycle Gangs and Mafia type organised crime groups including aboriginal groups and drug cartels. Aboriginal street gangs are not as highly organised as

other criminal organisations in Canada, but are some of the most violent. In Saskatchewan aboriginal gangs exist in Saskatoon and Regina. Saskatchewan had the highest concentration of gang membership in Canada. Winnipeg's gang activity also involves mainly First Nation gangs. The Canadian Criminal Intelligence Service (CISC), say that established, well-financed and connected Hong Kong Triad groups and crime syndicates are still, in their view, "the biggest long-term threat to Canadian law enforcement and society." In addition to Triad Societies, other Asian criminal groups, such as The Big Circle Gang, have also established national networks based in the major cities of Canada.

Among street gangs the 'Crips' and 'Bloods' both have adherents in several Montreal districts and are to be found also in Ottawa. The Greater Toronto Area has a very diverse range of gangs and in the mid 2000s police raids led to many gang members being deported back to Jamaica, Trinidad, Liberia, Sri Lanka, Colombia, Portugal, Somalia and others countries. Known crime groups in Vancouver include Indo-Canadian street gangs amongst many others and have a growing Mafia presence.

Various eastern European gangs known as 'bratvas' are also known to be active.

In Ontario, the R. v. Lindsay case in 2005 determined that the Hells Angels were a "criminal organisation" and that the Hells Angels were declared as a group, as opposed to individuals, to be a "criminal organisation". The Hells Angels are problematic because although they have been found by the courts to be a criminal organisation there is no official 'list' of such a finding. In other words, the existence of a particular group as a criminal organisation must be re-decided and proven in every new case. The Canadian Parliamentary Standing Committee on Justice and Human Rights was told by the police that, whilst they did not take issue with the criteria established for designating a group as a criminal organisation, they did take issue with the fact that once designated, it carries no weight in subsequent court cases. They gave the specific example of the Manitoba Chapter of the Hells Angels Motorcycle Club. This had been found by the Manitoba Court of Queen's Bench to be a criminal organisation, and yet in upcoming trials of Hells Angels members, this fact will have to be proved once again.

Illicit drugs continue to be the largest criminal market in Canada with 57% of the criminal marketplace being taken up by the drugs trade. The majority (83%) of organised crime groups are involved in the illicit drug trade, with other areas being human trafficking,

counterfeit products, illegal gambling, money laundering, and vehicle theft.

The predominant drug is cocaine, followed by cannabis, and then followed by synthetic drugs. One indication of the size of the drugs trade is that, in the Atlantic region, since 2008, the Canada Border Services Agency (CBSA) has seized more than C\$176 million in drugs arriving at Atlantic ports in sea containers. The majority of these drug seizures consist of hashish coming from Asia and Africa and cocaine arriving from South America. British Columbia has become the top destination for smuggling ketamine into Canada, much of it coming from Hong Kong and China. Ketamine hydrochloride, also known as "Special K", is a dissociative anaesthetic used in medicine and as a recreational drug. In March 2013 the CBSA said it had seized over C\$128 million worth of ketamine at B.C.'s border points over the past six years, a dollar value more than double that of ketamine seizures in Ontario and Quebec combined. Canada has also become a source country for synthetic drugs (like ecstasy and crystal meth) with groups smuggling in the precursor chemicals from source countries such as China and India. It also exports significant quantities of ecstasy and methamphetamine.

In 2011, the CISC reported that financial crime was about 11% of criminal market activity with Payment card fraud involving card thefts, fraudulent card applications, fake deposits, and skimming or counterfeiting.

Other criminal activity includes theft, contraband, alcohol and tobacco and human trafficking.

A recent example of the growing adaptability and co-operation is a case involving the Montreal Mafia, Hells Angels, aboriginal groups, New York Mafia and the Sinaloa Cartel. Jimmy Cournoyer from Quebec was the king pin of a massive international drug trafficking enterprise with ties to La Cosa Nostra, the Hells Angels and the Sinaloa Cartel in Mexico and was found guilty on April 3, 2013 to being the leader of a continuing criminal enterprise, conspiracies to manufacture, import and distribute marijuana, conspiracies to export and distribute cocaine, substantive and a conspiracy to launder money. Cournoyer was the principal leader of a Montreal-based drug distribution organisation affiliated with the Rizutto (Montreal Mafia) and Bonanno (New York Mafia) crime families, the Hells Angels and the Sinaloa Cartel. He had trafficked more than US\$1billion worth of marijuana, cocaine and ecstasy into the US between 1998 and 2012. His organisation transported tens of thousands of kilos of marijuana from outdoor growers in British Columbia to Montreal, Canada.

From there the drugs were smuggled into the US using transportation networks run by the Hells Angels. The drugs were smuggled through the Akwesasne Mohawk Reservation which straddles both sides of the U.S./Canadian border. Once the drugs were sold in the US, the organisation used the millions of dollars in drug proceeds to purchase cocaine from the Sinaloa Cartel in Mexico which was then distributed in Canada by the Rizzuto family. Cournoyer was also charged with witness tampering as he had also set up a C\$2mio "hit fund" set aside to murder any individuals who cooperated with the government. The agencies involved included various Regional and National and International Police forces from 3 countries, Border Patrols and the Akwesasne Mohawk Police Service and Akwesasne Tribal Police. The extent of corruption is still unknown but as an example several electricity linemen in British Columbia have been found guilty of providing 'alternative' electricity supplies for power hungry illegal hydroponic farms. Utility bills are not an issue for the criminals but they know that power consumption is monitored by the authorities.

Terrorism goes back a long way in Canadian history. Examples include the Sons of Freedom, a splinter group of the Doukhabor religious sect called the Freedomites who waged a sporadic 40 year campaign of bombing and burning against the State. Later on came the Front de Liberation du Quebec (FLQ) who tried to promote its objective of an independent Quebec. They executed a series of bombings against a range of targets, including the federal government, the post office, the armed forces, the RCMP, Canadian Broadcasting Corporation, Canadian National Railways and the Montreal Stock Exchange. Although the intent was usually to destroy property, at least six people died as a result of FLQ operations, and many others were severely injured. Canada's most deadly terrorist attack was the Air India attack when on June 23, 1985; a bomb exploded on Air India Flight 182 which was en route from Toronto to the UK. It killed all the 329 people aboard, most of whom were Canadians. The Air India bombing is still the worst terrorist attack in Canadian history. Today according to the Government of Canada in its 'Building Resilience Against Terrorism: Canada's Counter-terrorism strategy'(2011) 'Violent Islamist extremism is the leading threat to Canada's national security.' They say that several Islamist extremist groups have identified Canada as a legitimate target. In addition the document points out, 'violent "home-grown" Sunni Islamist extremists are posing a threat of violence. A recent example of home grown terrorism was early in 2013 when a couple John Nuttall and Amanda Korody, who are alleged to have placed a pressure cooker bomb to coincide with Canada Day (July 1ST) celebrations

at Victoria B.C. The bombs had been made safe by undercover officers prior to being planted Nuttall, a methadone addict had become a Muslim as had Korody. The term "Al-Qaeda inspired" was used to describe them but in fact it seems they are part of a growing group of marginalised inadequates whose motivation is not wholly ideological or religious. This makes them harder to discover.

As well as the threat of attacks on Canadian territory, groups and individuals have been identified within Canada who seek to carry out attacks on other states. Armenians, Tamil Tigers, Sikh separatists to name a few Yoav Lorbert Security Manager of El Al Israel Airlines in Toronto in 2012 said terror groups "don't want to cause a problem here""these groups attack for a reason and Canada is not an attractive target"they didn't attack Canada because it was a place to raise money and a safe haven for their families" and cell members send their families to live or attend school in Canada and don't want to cause problems.

Canada Designated Terrorist Organisations

Canada has listed the following Organisations as terrorist organisations.²⁸ These are: Abu Nidal Organisation; Abu Sayyaf Group; Al-Qaeda; Al-Qaeda in Iraq (AQI); Al-Qaeda in the Arabian Peninsula (AQAP); Al-Qaeda in the Islamic Maghreb (AQIM); Al-Shabaab; Al-Aqsa Martyrs' Brigade; Al-Gama'a al-Islamiyya; Al-Ittihad Al-Islam; Ansar al-Islam; Armed Islamic Group (GIA); Asbat Al-Ansar (AAA); Aum Shinrikyo; Autodefensas Unidas de Colombia (AUC); Babbar Khalsa International (BKI); Ejército de Liberación Nacional (ELN); Euskadi Ta Askatasuna (ETA); Fuerzas Armadas Revolucionarias de Colombia (FARC); Hamas; Haqqani Network; Harakat ul-Mujahidin (HuM); Hezb-e Islami Gulbuddin (HIG); Hezbollah; International Sikh Youth Federation; Islamic Army of Aden (IAA); Islamic Movement of Uzbekistan (IMU); Islamic Revolutionary Guard Corps' Qods Force; Jaish-e-Mohammed (JeM); Jemaah Islamiyah (JI); Kahane Chai; Kurdistan Workers Party (PKK); Lashkar-e-Jhangvi (LJ); Lashkar-e-Tayyiba (LeT); Liberation Tigers of Tamil Eelam (LTTE); Palestine Liberation Front (PLF); Palestinian Islamic Jihad (PIJ); Popular Front for the Liberation of Palestine - General Command (PFLP-GC); Popular Front for the Liberation of Palestine (PFLP); Sendero Luminoso (SL); Taliban; Tehrik-e-Taliban Pakistan (TTP); Egyptian Islamic Jihad; World Tamil Movement (WTM).

Mexico



Mexico is the site of several advanced Amerindian civilizations, including the Maya, and Aztec. Mexico was conquered and colonized by Spain in the early 16th century and achieved its independence in 1821. The country is named after its main city itself

the centre of the Aztec empire, or Mexihco named after the god of war and patron of the Aztecs. The history of Mexico, a country situated in the southern portion of North America, is at once a record of great cultural achievement and a catalogue of violent military and political struggle.

During the Mexican-American War, from 1846 to 1848, the US annexed Texas, which Mexico considered part of its territory, then conquered New Mexico and California. The Mexican Revolution in 1910, culminated with the promulgation of the 1917 Constitution and the emergence of the country's current political system, which was dominated by the Institutional Revolutionary Party (PRI) until 2000 when, for the first time an opposition party (The National Action Party) won the presidency, though recent elections held in 2012, resulted in the PRI returning the power, via President Pena Nieto.

Over a century ago, the Mexican dictator Porfirio Díaz famously exclaimed: 'Pobre Mexico! tan lejos de Dios, tan cerca de los Estados Unidos' Poor Mexico! So far from God, so close to the US. The quote today epitomises the challenges for México with the murderous criminal violence that is intertwined with the trafficking of drugs mainly to its Northern neighbour due to the insatiable demand for the drugs which in turn fuels that violence.

Mexico's geographical position set between the world's largest cocaine producers and one of the world's biggest consumers of cocaine making it a logical transit route for the product. Mexican Drug Trafficking Organisations (DTOs) are essentially transport and logistics organisations who are competing for the business of supplying the US with marijuana and cocaine supplied by indigenous, Central American and South American producers, and, in the case of Ephedra based products; China.

This trafficking generates vast amounts of money with estimates of up to US\$25-US\$30bio worth of illegal drugs coming through Mexico into the US. Earlier US efforts to interdict Colombian Caribbean drugs routes that went directly to the US had a degree of success, but led to unintended consequence. The creation of Mexico as a transhipment point for cocaine destined for the US allowed the Mexican cartels to evolve into the powerful DTOs they are today.

The DTOs are located in specific geographic areas within Mexico and many have set up logistics and distribution networks in US cities. Some, such as Los Zetas have 'backwardly integrated' by becoming established in Guatemala. The Cartels are located in those areas along Mexico's border with the US and in its Gulf, Caribbean and Pacific ports. Some are also located on the connecting highway routes between these points. These location and structures are predicated on the notion of who controls the trade routes into Mexico, through it, and on to the US.

In effect the groups have divided large tracts of Mexico into "fiefdoms" This can be illustrated by using examples of just two of the cartels. The Gulf Cartel, located in the city of Reynosa controls Tamaulipas state, parts of Nuevo Leon state and similarly Veracruz state. It also borders with the US. More importantly it controls the ports of Tampico and Veracruz. The Sinaloa federation's capital city is Culiacan and also shares a border with the US. Its territory consists of Sinaloa and Sonora states and controls the port cities of Puerto Vallarta, Manzanillo and Mazatlan. Cartels close to the borders also seek to have relationships back down the supply chain with cartels in (for example) the Guerrero-Michoacán (Pacific) "fiefdoms" and the Yucatan (Caribbean /Gulf of Mexico) "fiefdoms".

Mexican cartels are also increasing their relationships with prison and street gangs in the US in order to push market distribution. A US Congressional report noted that gangs such as the Latin Kings and Mara Salvatrucha (MS-13) buy bulk methamphetamine from Mexican drug cartels for resale. Again, according to the FBI, Mexican cartels focus only on wholesale distribution, leaving retail sales of drugs to the street gangs. The cartels will sell to all and any gangs but do not take sides in US gang turf wars.

The routes used to ship drugs from South America to the US are also used for Human Smuggling and Trafficking. They are also used in the reverse direction to supply producers with precursor chemicals, arms and counterfeit goods from China.

The DTOs compete to protect or increase market share and sometimes in resisting governmental interdiction efforts and this often turns into bloodshed. According to Mexico's 'Reforma'²⁹ newspaper, there were 11,583 drug-related murders in Mexico in 2010, compared with 6,587 in 2009. DTOs increasingly employ military tactics and use heavy weaponry such as sniper rifles, grenades, and rocket-propelled grenades in attacks on government security personnel as well as IEDs against local officials.

The Mexican DTOs have also moved into piracy, prostitution and the theft of oil and minerals. The theft of minerals in the western state of Michoacan has increased with the cartel known as La Familia Michoacana which was found to have sold 1.1 million tons of illegally extracted iron ore in China for US\$42mio. Some authorities suggest that the DTOs are buying up small and medium sized mines to launder money.

The oil industry has also been affected with one example being the State energy company Petroleos Mexicanos (PEMEX) which had US\$300mio worth of natural gas condensate stolen by Los Zetas members. On 1 June 2011, Pemex filed a lawsuit accusing nine US companies of colluding with criminals linked to the drug trade to sell an estimated US\$300mio worth of stolen oil since 2006. That almost equals the cocaine market in Mexico. Clearly if all narcotics vanished tomorrow the DTOs would have no problem finding new revenue streams.

According to the Institute for the Protection of Intellectual Property Mexico is the fourth largest producer and consumer of counterfeited and pirated products worth US\$12.5bio a year. In Mexico, shoppers can buy Arizona Cardinals jerseys for US\$25, less than a third of what an NFL original costs. There are fake Sony televisions, counterfeit Nike shoes and proprietary whiskey brands. Adobe Photoshop, which costs US\$650 in the US, can be bought outside Computer Plaza in Mexico City for 40 pesos, or US\$. Two of every three pairs of tennis shoes sold are counterfeit, whilst about 65% of DVDs and CDs are pirated. According to the Washington based International Intellectual Property Alliance. Mexican buyers account for 9% of all pirated US goods sold worldwide. Again according to the US National Public Radio Network, Mexico's multibillion-dollar pirated goods market is worth more than its oil exports and illicit narcotics trade combined.

Attempts to prosecute are politically contentious in Mexico because many street vendors who sell counterfeit goods are people who cannot find regular jobs. In all, about 1.9 million of Mexico's 42.3 million workers are

street vendors, part of the "informal" economy.

Much of the data about piracy is reporting the views of trade groups and business interests and much of that is anecdotal or 'guesimates'. However, one piece of hard research was produced by the Social Science Research Council (US University body) entitled 'Media Piracy in Emerging Economies'. This poured water on the claims of the industry bodies with regard to the piracy of electronic media and in particular the claim that the counterfeiters were linked to the Drug Cartels.

Money laundering by the DTOs is carried out through a vast range of business entities such as construction and real estate companies. With regard to laundering drug proceeds the preferred methods of smuggling US currency into Mexico (and the repatriation of funds into the US) is by bulk shipments via couriers, use of armoured vehicles, and wire transfers. Bulk Cash shipments and couriers across all borders extend the laundering into Central America where the process of laundering is even easier.

Remittance systems have also been shown to be vulnerable. Mexico has a sophisticated financial sector, a large cash-based informal sector, and inadequately enforced regulatory controls. According to US authorities, drug trafficking organisations send between US\$19 and US\$29bio annually to Mexico from the US. The Mexican government has seized over US\$457.5mio in bulk currency shipments since 2002. Again, bulk-cash seizures in 2010 totalled US\$32.4mio.

Wachovia Bank (now part of Wells Fargo), was fined US\$160mio in March 2010 for failing to monitor money flows from Casa de Cambios in particular and HSBC was soon to follow being fined US\$1.96bio for numerous money laundering and sanctions failures including failing to control payment flows from Casa de Cambio's in Mexico. The Casa de Cambio that hit the headlines and links both the Wachovia case and that of HSBC is the Casa de Cambio Puebla. For more details on each see Part 2, Section 7, Criminal Cases and Section 8, Enforcement Cases below.

Following these high profile cases and penalties imposed, the number of casa de cambios has declined but there are over 4000 centros cambiarios, which are largely unregulated, and approximately 1200 registered money transmitters. Commercial banks, foreign exchange companies, and general commercial establishments in Mexico also offer money exchange services. For more details see Part 1, Section 2, Sub-section 2, Money Services Businesses above.

Special Focus 15

Mexican Drug Trafficking Organisations (DTOs)



Mexican criminal gangs, known as cartels, the best known, still enduring and most successful of which are the **Sinaloa Cartel**, **Los Zetas**, **Gulf Cartel**, **Tijuana Cartel**, **Beltrán Leyva Cartel**, **Juárez Cartel** and the **Knights Templar Cartel**, each control large swaths of

Mexican territory and dozens of municipalities. The cartels are currently waging violent turf battles over control of key smuggling corridors through Mexico and defending themselves from government action. The **Sinaloa Cartel** is considered the largest and most powerful drug trafficking organisation in the world and fugitive Joaquín Archivaldo Guzmán Loera is its leader. Known as "El Chapo Guzmán" ("Shorty Guzmán") for his 1.68 m (5 ft 6 in) stature, he became Mexico's top drug kingpin in 2003 and is now considered, "the most powerful drug trafficker in the world," by the US Department of the Treasury.³⁰ **Los Zetas** is considered the most violent.

The US Drug Enforcement Administration reports that the Mexican drug cartels operating today are far more sophisticated and dangerous than any other organised criminal group in US law enforcement history. The cartels use grenade launchers, automatic weapons, body armour, and sometimes Kevlar helmets. Casualty numbers have escalated significantly over time. According to a Stratfor report, the number of drug-related deaths in 2006 and 2007 (2,119 and 2,275) more than doubled to 5,207 in 2008. The number further increased substantially over the next two years, from 6,598 in 2009 to over 11,000 in 2010.

There were no cartels in the 1980s in Mexico, as the entire business was controlled by one man, **Félix Gallardo** who was known as the "Godfather". He oversaw all operations and he bought protection by bribing the police and politicians. Miguel Angel Félix Gallardo was a former Mexican Judicial Federal Police agent, who started off by smuggling marijuana and opium into the US, and was the first Mexican to link up with Colombia's cocaine cartels in the 1980s. This was easily accomplished because Félix Gallardo had

already established an infrastructure that stood ready to serve the Colombia-based traffickers. By the 1980s he controlled all illegal drug trade in Mexico and the corridors across the Mexico-USA border. "The Godfather" then decided to divide up the trade he controlled as it would be more efficient and less likely to be brought down in one law enforcement swoop. In a way, he was privatizing the Mexican drug business while sending it back underground, to be run by others who were less well known or not yet known by the US DEA. Félix Gallardo convened the nation's top drug traffickers at a house in Acapulco where he allocated either territories or routes, for example, the **Tijuana route** would go to the **Arellano Felix brothers**, the Ciudad Juárez route would go to the **Carrillo Fuentes family**. Miguel Caro Quintero would run the **Sonora corridor**. The control of the Matamoros, Tamaulipas corridor - which would become the **Gulf Cartel** - would be controlled by Juan García Abrego. Meanwhile, Joaquín Guzmán Loera and Ismael Zambada García would take over Pacific coast operations, becoming the **Sinaloa Cartel**. Guzmán and Zambada brought veteran Héctor Luis Palma Salazar back into the fold. Félix Gallardo still planned to oversee national operations, as he maintained important connections, but he would no longer control all details of the business. Félix Gallardo was finally arrested on 8 April 1989.

Mexico is still the main foreign supplier of cannabis and a major supplier of methamphetamine to the US. Almost half the cartels revenue comes from cannabis. Although Mexico accounts for only a small share of worldwide heroin production, it supplies a large share of the heroin distributed in the US. Drug cartels in Mexico control approximately 70% of the foreign narcotics that flow into the US. The US State Department estimates that 90% of cocaine entering the US transits through Mexico, with Colombia being the main cocaine producer, followed by Bolivia and Peru.

The drug trade is supplemented with many other lucrative criminal activities, including human trafficking and people smuggling, that has made the Mexican gangs so successful and induced them to fight each other for control of territory and with the State government.

In 2006, former Mexican president Felipe Calderón launched a massive crackdown against drug trafficking organisations, in conjunction with the US. Since then, more than 40,000 people have been killed in drug-related violence. While the US has supplied funding and labour to increase Mexico's institutional capacity to address drug trafficking, its primary focus has been on cross-border policing and targeting US drug users. Enrique Peña Nieto, who succeeded Calderón as

President in December 2012, has announced intentions to shift Mexico's drug war strategy to quell violence against civilians rather than targeting cartel leaders.

Following the establishment of the Mexican cartels by Félix Gallardo and with his arrest, the balance of power between the various Mexican cartels shifted as new ones emerged and older ones weakened and collapsed. A disruption in the system, such as the arrests or deaths of cartel leaders, generates bloodshed as rivals move in to exploit the power vacuum. Leadership vacuums sometimes are created by law enforcement successes against a particular cartel, thus cartels often will attempt to use law enforcement against one another, either by bribing Mexican officials to take action against a rival or by leaking intelligence about a rival's operations to the Mexican government or the US Drug Enforcement Administration.

The reasons for the escalating violence involving the Mexican Cartels are complex but have their roots in the unravelling of a long-time implicit arrangement between narcotics traffickers and governments controlled by the Institutional Revolutionary Party (PRI), which began to lose its grip on political power starting in the late 1980s including during the infamous Presidency of Carlos Salinas (see Part 2, Section 7, Criminal Cases for the case of **Raúl Salinas**) and ending with the election of the independent Presidency of Vincent Fox in 2000 and culminating in the Presidency and action taken by President Calderón from 2006. Whilst fighting between rival drug cartels began in earnest after the 1989 arrest of Miguel Ángel Félix Gallardo, there was then a lull in the fighting during the late 1990s but the violence steadily worsened since 2000. The then President Vicente Fox sent small numbers of troops to the US-Mexico border to fight the cartels with little success.

President Calderón was more aggressive, and he sent for example 6,500 federal troops to the state of Michoacán to end drug violence there. As time progressed, Calderón continued to escalate his anti-drug campaign, in which there were now about 45,000 troops involved in addition to state and federal police forces. In 2010 Calderón said that the cartels seek "to replace the government" and "are trying to impose a monopoly by force of arms, and are even trying to impose their own laws."³¹ The challenges faced by the government remain formidable however. For example in 2008, General Sergio Aponte, the man in charge of the anti-drug campaign in the state of Baja California, made a number of allegations of corruption against the police forces in the region. Among his allegations, Aponte stated that he believed Baja California's anti-kidnapping squad was actually a kidnapping team working in

conjunction with organised crime, and that bribed police units were being used as bodyguards for drug traffickers. These accusations of corruption suggested that the progress against drug cartels in Mexico has been hindered by bribery, intimidation, and corruption.

On April 26, 2008, a major battle took place between members of the **Tijuana** and **Sinaloa Cartels** in the city of Tijuana, Baja California, which left 17 people dead. The battle also caused concern about the violence spilling into the US, as Tijuana and a number of other border cities became hotspots for violence in the war. In September 2008, grenade attacks in Morelia by suspected cartel members killed eight civilians and injured more than 100. In March 2009, President Calderón called in an additional 5,000 Mexican Army troops to Ciudad Juárez. The US Department of Homeland Security has also said that it considered using the National Guard to counter the threat of drug violence in Mexico from spilling over the border into the US. The governors of Arizona and Texas asked the federal government to send additional National Guard troops to help those already there supporting local law enforcement efforts against drug trafficking.

The Mexican attorney general's office says that 9 of 10 victims are members of organised crime groups, and deaths among military and police personnel are an estimated 7% of the total. The states that suffer from the conflict most are Baja California, Guerrero, Chihuahua, Michoacán, Tamaulipas, Nuevo León and Sinaloa. Whilst the Calderón administration has been successful in damaging the Cartels, the country's security situation continued to seriously deteriorate with the total number of drug-related homicides continuing to climb steeply. Violence escalated with intimidation and fear. The discovery of hit lists with the names of police officers had become increasingly common in many Mexican cities along the US border. It also is common for the officers named on those lists to be gunned down one by one. In addition, drug trafficking organisations began displaying large banners over highways in cities around the country. Many of the banners make threats against rivals, or accuse a particular criminal group of being supported by local and federal government officials. In several cases, purported recruiting banners appeared in northern Mexico offering higher pay and better equipment to soldiers and police officers who defect to **Los Zetas**.

One escalation in this conflict is the traffickers' use of new means to claim their territory and spread fear. Cartel members have broadcast executions on YouTube, tossed body parts into crowded nightclubs and hung banners on streets. In 2008 Morelia grenade attacks

took place, when two hand grenades were thrown onto a crowded plaza, killing ten people and injuring more than 100. Some see these efforts as intended to sap the morale of government agents assigned to crack down on the cartels; others see them as an effort to let citizens know who is winning the war. The extreme violence attacks foreign investment in Mexico, and the Finance Minister, Agustín Carstens, said that the deteriorating security alone is reducing gross domestic product annually by 1% in Mexico, Latin America's second-largest economy.

Improved cooperation of Mexico with the US led to the recent arrests of 755 Sinaloa Cartel suspects in US cities and towns, but the US market is being eclipsed by booming demand for cocaine in Europe, where users now pay twice the going US rate.

In December 2010 the government of Spain remarked that Mexican cartels have multiplied their operations in that country, becoming the main entry point of cocaine into Europe.

The Mexican Army crackdown has driven some cartels to seek a safer location for their operations across the border in Guatemala, attracted by corruption, weak policing and its position on the overland smuggling route. The smugglers pick up drugs from small planes that land at private airstrips hidden in the Guatemalan jungle. The cargo is then moved up through Mexico to the US border. Guatemala has also arrested dozens of drug suspects and torched huge cannabis and poppy fields, but is struggling.

In February 2009, Los Zetas Cartel threatened to kill the President of Guatemala, Álvaro Colom. On March 1, 2010, Guatemala's chief of national police and the country's top anti-drugs official have been arrested over alleged links to drug trafficking. A report from the Brookings Institution warns that, without proactive, timely efforts, the violence will spread throughout the Central American region.

At least nine Mexican and Colombian drug cartels have established bases in West African nations. They are reportedly working closely with local criminal gangs to carve out a staging area for access to the lucrative European market.

The Colombian and Mexican cartels have discovered that it is much easier to smuggle large loads into West Africa and then break that up into smaller shipments to Europe, mostly Spain, the UK and France. Higher demand for cocaine in Western Europe in addition to North American interdiction campaigns has led to

dramatically increased trafficking in the region: nearly 50% of all non-US bound cocaine, or about 13% of all global flows, is now smuggled through West Africa.

The US Justice Department considers the Mexican drug cartels as the greatest organised crime threat to the US. During the first 18 months of Calderón's presidency, the Mexican government has spent about US\$7bio in the war against drugs. In seeking partnership from the US, Mexican officials point out that the illicit drug trade is a shared problem in need of a shared solution, and remark that most of the financing for the Mexican traffickers comes from American drug consumers.

On 25 March 2009, former US Secretary of State Hillary Clinton, stated that "Our [America's] insatiable demand for illegal drugs fuels the drug trade", and that "the US bears shared responsibility for the drug-fuelled violence sweeping Mexico."³² US State Department officials are aware that Mexican President Felipe Calderón's willingness to work with the US is unprecedented on issues of security, crime and drugs, so the US Congress passed legislation in late June 2008 to provide Mexico and Central American countries with US\$1.6bio for the Mérida Initiative, a three-year international assistance plan.

The Mérida Initiative provided Mexico and Central American countries with law enforcement training and equipment, as well as technical advice to strengthen the national justice systems. The Mérida Initiative did not include cash or weapons. In January 2009, a US military assessment expressed some concern that if the war is extended 25 years, it could cause a collapse of the Mexican government due to the military strength of organised crime, and that the conflict could possibly spread to border states.

Currently, the Mexican drug cartels already have a presence in most major US cities. In 2009, the Justice Department has reported that Mexican drug cartels have infiltrated nearly 200 cities across the US, including Los Angeles, Chicago and Atlanta.

In March 2009, the Obama administration outlined plans to redeploy more than 500 federal agents to border posts and redirect US\$200mio to combat smuggling of illegal drugs, money and weapons.

In May 2010 President Obama authorized deployment of 1,200 National Guard troops to the US border with Mexico to assist with border protection and enforcement activities, as well as help train additional Customs and Border Protection agents. The deployment drew criticism primarily from the border state governments which argued that an additional 1,800

men to control over 2,000 miles of border is not nearly enough and is more a political show than a serious attempt to stop incursions at the border.

Despite the fact that Mexican drug cartels and their Colombian suppliers generate, launder and remove US\$18bio to US\$39bio from the US each year, the US and Mexican governments have been criticized for their response to confront the various cartels' financial operations, including money laundering.

The US Drug Enforcement Administration (DEA) has identified the need to increase financial investigations relating to the movement of illegal drug funds to Mexico. The DEA states that attacking the financial infrastructure of drug cartels has to play a key role in any viable drug enforcement strategy. However, the US DEA has noted that the US and Mexican financial services industry continues to be abused for drug money movement (see Part 2, Section 8, Wachovia, American Express and HSBC cases where drug money flowed through these institutions and each was subsequently fined by US authorities for having lax money laundering controls).

In 2010 President Felipe Calderón proposed sweeping new measures to crack down on the cash smuggling and money laundering. Calderón limited foreign exchange cash transactions to US\$1,500 per person per month and cash bank deposits to US\$4,000 per month and, taking effect in 2013, banned cash, purchases of real estate and of certain luxury goods that cost more than 500,000 pesos (about US\$38,750). His package also required businesses to report large transactions, such as real estate, jewellery and purchases of armour plating above these limits.

Finally FIs are required to report monthly credit card balances over 50,000 pesos (US\$3,875). Mexico appears to be following Spain and Italy in this regard who already ban large cash transactions above €1,000 respectively.

Following the election in 2012 of President Enrique Pena Nieto, some commentators claimed the new President would attempt a much less aggressive attitude towards the cartels, some even suggesting the possibility of seeking an arrangement of sorts in order to reduce the level of violence. There has to date been little evidence of any such approach though it is thought that the new President will seek to frame the problem as a more traditional law enforcement problem and reduce the involvement of the army which may in fact reduce the violence.

The Leading Mexican Cartels

Whilst the 5 original Mexican cartels created by Felix Gallardo in the 1980s remain, two have merged, one has split, and some new ones have emerged and been disbanded. This as a result of the wars between them and between them and the Federal government which will continue to change the Mexican criminal landscape. The original cartels were established around 5 existing routes and corridors so: (i) the Tijuana Cartel would go to the Arellano Felix brothers; (ii) the Ciudad Juárez route would go to the Carrillo Fuentes family; (iii) the Sonora corridor would go to Miguel Caro Quintero; (iv) the Matamoros, Tamaulipas corridor, then becoming the Gulf Cartel would go to Juan García Abrego and (v) the Sinaloa Cartel on the pacific coast would go to Joaquín Guzmán Loera and Ismael Zambada García.

Since then the Sonora Cartel has merged into the Gulf Cartel split creating La Familia (The Michoacan Family) which has since disbanded and been replaced with the Knights Templar Cartel but more importantly the Gulf Cartel's military wing also split and is now a major rival and is known as Los Zetas. The Beltrán Leyva brothers were able to establish themselves exploiting the crises around the Gulf Cartel.

Since February 2010, the major cartels have aligned together into two factions, one integrated by the Juárez Cartel, Tijuana Cartel, Los Zetas Cartel and the remnants of the Beltrán-Leyva Cartel, with Los Zetas being the most powerful and the other faction integrated by the Gulf Cartel, Sinaloa Cartel and Knights Templar Cartel with the Sinaloa Cartel of these the most powerful.

Gulf Cartel - Mexico

The Gulf Cartel (Cartel del Golfo), based in Matamoros, Tamaulipas, has been one of Mexico's two dominant cartels in recent years. In the late 1990s, it hired a private mercenary army (an enforcer group now called Los Zetas), which in 2006 stepped up as a partner but, in February 2010, their partnership was dissolved and both groups engaged in widespread violence across several border cities of Tamaulipas state, turning several border towns into "ghost towns".

The Gulf Cartel (CDG) was strong at the beginning of 2011, holding off several Los Zetas incursions into its territory. However, as the year progressed, internal divisions led to intra-cartel battles in Matamoros and Reynosa, Tamaulipas state. The infighting resulted in several arrests and deaths in Mexico and in the US. The CDG has since broken apart, and it appears that one faction, known as Los Metros, has overpowered its rival Los Rojos faction and is now asserting its control

over CDG operations. The infighting has weakened the CDG, but the group seems to have maintained control of its primary smuggling corridors, into the US.

Juárez Cartel - Mexico

The Juárez Cartel controls one of the primary transportation routes for billions of dollars worth of illegal drug shipments annually entering the US from Mexico. Since 2007, the Juárez Cartel has been locked in a vicious battle with its former partner, the Sinaloa Cartel, for control of Ciudad Juárez.

La Línea is a group of Mexican drug traffickers and corrupt Juárez and Chihuahua state police officers who work as the armed wing of the Juárez Cartel. Vicente Carrillo Fuentes headed the Juárez Cartel but was captured in 2009. Following his capture, the Juárez Cartel continued to weaken, however, it still controls the three main points of entry into El Paso, Texas. The Juárez Cartel is only a shadow of the organisation it was a decade ago, and its weakness and inability to effectively fight against Sinaloa's advances in Juárez contributed to the lower death toll in Juárez in 2011.

Sinaloa Cartel - Mexico

The Sinaloa Cartel sometimes known as the "Pacific Cartel", and headed by Joaquín "El Chapo" Guzmán, began to contest the Gulf Cartel's domination of the coveted southwest Texas corridor following the arrest of Gulf Cartel leader Osiel Cárdenas in March 2003.

The Sinaloa cartel used to be known as La Alianza de Sangre ("Blood Alliance") and grew as a result of a 2006 accord between several groups located in the Pacific state of Sinaloa. In February 2010, new alliances were formed against Los Zetas and Beltrán Leyva Cartel. As of May 2010, numerous reports by Mexican and US media claimed that Sinaloa had infiltrated the Mexican federal government and military, and colluded with it to destroy the other cartels. The Colima, Sonora and Milenio Cartels are now branches of the Sinaloa Cartel.

The cartel is considered the largest and most powerful drug trafficking organisation in the world and fugitive Joaquín Archivaldo Guzmán Loera is its leader. Known as "El Chapo Guzmán" ("Shorty Guzmán") for his 1.68m (5ft 6in) stature, he became Mexico's top drug kingpin in 2003 after the arrest of his rival Osiel Cárdenas of the Gulf Cartel and is now considered "The most powerful drug trafficker in the world," by the US Department of the Treasury. Guzmán Loera has been ranked by Forbes magazine as one of the most powerful people in the world every year since 2009; ranking 41st, 60th and 55th respectively. He was also listed by Forbes as the 10th richest man in Mexico (1,140th in the

world) in 2011, with a net worth of roughly US\$1bio. Forbes also calls him the "biggest druglord of all time", and the DEA strongly believes he has surpassed the influence and reach of Pablo Escobar, and now considers him "the godfather of the drug world." Guzman Loera's Sinaloa Cartel smuggles multi-ton cocaine shipments from Colombia through Mexico to the US, and has distribution cells throughout the US. The organisation has also been involved in the production, smuggling and distribution of Mexican methamphetamine, marijuana, and heroin.

The US offers a US\$5mio reward for information leading to his capture. The Mexican government offers a reward of 30mio pesos for such information. Guzmán was captured in Guatemala in 1993 and extradited to Mexico, where he was jailed in a maximum security prison, but in 2001, Guzmán escaped in a laundry basket and resumed his command of the Sinaloa Cartel. Guzmán has one close associate, Ismael Zambrano García who is also a fugitive. It is thought that Guzman is hiding in the towering Sierra Madre mountains.

Tijuana Cartel - Mexico

The Tijuana Cartel, also known as the Arellano Felix Organisation, was once among Mexico's most powerful. It is based in Tijuana, one of the most strategically important border towns in Mexico, and continues to export drugs even after being weakened by an internal war in 2009. Due to infighting, arrests and the deaths of some of its top members, the Tijuana Cartel is a fraction of what it was in the 1990s and early 2000s. After the arrest or assassination of various members, the cartel is currently headed by Luis Fernando Sánchez Arellano, a nephew of the Arellano Felix brothers.

La Familia Michoacana (Disbanded) - Mexico

The Michoacana Family or LFM was a Mexican drug cartel and an organised crime syndicate based in the Mexican state of Michoacana. Formerly allied to the Gulf Cartel, as part of Los Zetas it split off in 2006. The cartel's first leader, Nazario Moreno González, was known as El Más Loco (The Craziest One). Since 2009 under pressure from the Federal Government, LFM offered to disband their cartel provided the government ended their military involvement in Michoacana state. This was rejected and ended with first the killing of its founder and leader Nazario Moreno González, which contributed significantly to the Mexican Federal Police declaring in 2011, that LFM cartel had been disbanded.

Knights Templar - Mexico

The Knights Templar drug cartel (Spanish: Caballeros Templarios) was created in Michoacana in March 2011 after the death of the charismatic leader of La

Familia Michoacana Cartel, Nazario Moreno González. The Cartel is headed by Enrique Plancarte Solís and Servando Gómez Martínez who formed the Knights Templar due to differences with José de Jesús Méndez Vargas, who had assumed leadership of La Familia Michoacana. After the emergence of the Knights Templar, sizable battles flared up during the spring and summer months between the Knights Templar and La Familia. The organisation has grown from a splinter group to a dominant force over La Familia, and it appears to be taking over the bulk of their original operations in Mexico. At present, the Knights Templar appear to have aligned with the Sinaloa Cartel in an effort to root out the remnants of La Familia and to prevent Los Zetas from gaining in the region.

Beltrán Leyva Cartel (Disbanded) - Mexico

The Beltrán Leyva Cartel was a Mexican drug cartel and organised crime syndicate founded by the four Beltrán Leyva brothers: Marcos Arturo, Carlos, Alfredo and Héctor. In 2004 and 2005, Arturo Beltrán Leyva led powerful groups of assassins to fight for trade routes in northeastern Mexico for the Sinaloa Cartel. Through the use of corruption and intimidation, the Beltrán Leyva Cartel was able to infiltrate Mexico's political, judicial and police institutions to feed classified information about anti-drug operations, and even infiltrated the Interpol office in Mexico.

The Mexican Federal Police considers the cartel to have been disbanded, and the last cartel leader, Héctor Beltrán Leyva, apparently has been inactive and remains a fugitive, with a US\$5mio bounty from the US and US\$2.1mio bounty from Mexico on his head.

Los Zetas Cartel - Mexico

Los Zetas were led until recently by Heriberto "El Lazca" Lazcano and are considered by the US DEA as the most violent paramilitary enforcement group in Mexico. The Zetas is a criminal organisation dedicated mostly to the international illegal drug trade, assassinations, extortion, kidnapping and other organised crime activities.

This drug cartel was founded by a group of former Mexican Army Special Forces deserters and now it includes corrupt former federal, state, and local police officers, as well as ex-Kaibiles from Guatemala. This group of highly trained gunmen was first hired as a private mercenary army and bodyguard troupe for Mexico's Gulf Cartel. After the arrest of the Gulf Cartel's leader, Osiel Cárdenas Guillen, as well as other events, the two entities became a combined trafficking force, with Los Zetas taking a more active leadership role in drug trafficking.

Since February 2010 Los Zetas have gone independent and became enemies of its former employer/partner, the Gulf Cartel. In response to such aggressive efforts on the part of the Zetas to defend and control its smuggling corridors to the US, the rival Sinaloa Cartel established its own heavily armed enforcer gang, Los Negros. The group operates in a similar fashion to Los Zetas, but with less complexity. Los Zetas have set up camps to train recruits as well as corrupt ex-federal, state, and local police officers.

In September 2005 testimony to the Mexican Congress, then-Defence Secretary Clemente Vega indicated that the Zetas had also hired at least 30 former Kaibiles from Guatemala to train new recruits because the number of former Mexican special forces men in their ranks had shrunk. Los Zetas' training locations have been identified as containing the same items and setup as special forces training facilities.

Los Zetas are primarily based in the border region of Nuevo Laredo, with hundreds more throughout the country. In Nuevo Laredo it is believed they have carved the city into territories, placing lookouts at arrival destinations such as airports, bus stations and main roads.

In addition to conducting activities along the border, they are visible throughout the Gulf Coast region, in the Southern states of Tabasco, Yucatan, Quintana Roo, and Chiapas, and in the Pacific Coast states of Guerrero, Oaxaca and Michoacana, as well as in Mexico City. Evidence also indicates that they may be active in Texas, other US states and in Italy with the Ndrangheta.

Former leader Heriberto Lazcano was killed by Mexican marines in a shootout in 2012 in a small town in northern Mexico, 130 miles from the Texas border. In a twist, a group of armed men later stole Lazcano's body from a funeral home. His successor Miguel Trevino Morales was arrested in July 2013 dealing another significant blow to Los Zetas. It remains unknown as to both who now leads the organisation and whether the senior decapitations will materially affect the success of this criminal organisation.

Caribbean



The Caribbean islands are strewn across an arc of more than 2,000 miles with over 7,000 islands and are made up of 13 sovereign states and 17 dependent territories the area is a microcosm of the colonial history of Europe and more recent US history. Whilst the Caribbean countries are

all islands many are for all practical purposes linked to the South American mainland States, the Central American mainland and that of North America.

In effect the Caribbean is a series of stepping stones geographically placed along the world's major drug and cash highway between the world's major source of cocaine and the world's largest markets of consumers. In many cases this colonial past has fostered a diaspora of people with links to European markets who can move in both directions. Marijuana is also a major exported crop but market forces have created competition in the form of European and US home grown sinsemilla with estimates that up to 50% of high strength cannabis could be 'home grown'.

In 2009 a Ministerial conference was held consisting of the Heads of State of: Antigua and Barbuda, Bahamas, Belize, Cuba, Dominican Republic, Grenada, Haiti, Jamaica, St Vincent and the Grenadines, St Kitts and Nevis, Saint Lucia, Suriname and Trinidad and Tobago. At the conference they affirmed a Declaration on Combating Drug Trafficking, Organised Crime and Terrorism which they declared were challenges for Security and Development in the Caribbean. In particular they identified a list of pressing problems including light weapons and drugs trafficking with related criminality, terrorism financing and transnational organised crime. Financial crime particularly money laundering were seen also to be major problems.

Corruption in the Caribbean varies from country to country but is in general pervasive and high. Each country has linguistic, historical commercial and sometimes even legal ties to some of the major European consumers strengthened by daily air flights and sea container traffic.

There are also many people originating from Caribbean countries who play a part in drug distribution in Europe and the US.

The flows of drugs create many return flows of drug revenues that need laundering and throughout the area remittances from expatriates along with many financial

services industries create the conditions and cover for some money laundering.

In spite of decades of combatting drugs by these countries along with the US the production and trafficking of cocaine, marijuana, heroin, and methamphetamine still unabatedly generate a multi-billion dollar black market in which Drug Trafficking Organisations (DTOs) have thrived.

The very authority of some Caribbean states is being challenged in those transit countries where the governments are too often fragile and corruptible. The Caribbean Basin Security initiative along with others in the region (Plan Colombia; Merida Initiative; CARSI) are all ostensibly working to support the rule of law and anti-corruptions measures. Whilst the US /Mexican land border now predominates as the main route for Andean cocaine the growing European markets still use routes via the Caribbean and Jamaica is a major exporter of cannabis to the US.

The Caribbean - South Florida route into the US had seen some decline recently as alternatives open up but some experts are suggesting that this route will start to see rapid growth again. Indeed Dominican and Puerto Rican groups are competing on price asking Colombian traffickers for a little as half that normally charged by the Mexicans.

Of the 16 countries in the Caribbean area four have been identified by President Obama as major drug producing or transit countries. These are Haiti and the Dominican Republic; Jamaica and the Bahamas.

The President annually issues a Presidential determination identifying which countries are regarded as drug majors. Of the 20 countries in the world identified five of them have been Caribbean countries and have been on that list for the past ten years. Pointing this up a former DEA Chief of Operations described the Dominican Republic as a "command control and communications centre "for Caribbean drug operations. Despite their diversity, one thing all Caribbean countries have in common is that they suffer greatly from the supply of drugs from the south and the demand to the north.

Historically, the Caribbean has also been susceptible to money laundering for several reasons. Many small Caribbean nations (some very small) began providing offshore financial services for the western world's much bigger economies as a way to gain economic benefits for their own resource poor countries. Due to their small state institutional capacity and often coupled with political corruption they did not have the ability to carry out proper oversight of these services whilst finally tourism created many cash-based enterprises through which dirty money can move.

Bahamas

Following the arrival of Christopher Columbus, thought to have sighted and landed in San Salvador, meeting local Lucayan Indians, which is today one of the many islands of the Bahamas in 1492, the islands in and around surrounding San Salvador (or Christ the Saviour). The name Bahamas also comes from Columbus, from the Spanish word "baja mar" meaning shallow sea. The Bahamas was inhabited by a British settlement in 1647. The islands became a colony in 1783 and independent country in 1973. It has prospered through tourism and developed a successful offshore financial centre and has established a large free trade zone at Freeport harbour.

The Bahamas is not a significant drug producing country but remains a transit point for illegal drugs bound for the US and other international markets. The Bahamas' close proximity to the coast of Florida as well as Caribbean drug transshipment routes makes it a natural conduit for drug, cigarette and arms smuggling and bulk cash movements. Furthermore, the Bahamas's 700 islands and cays, the vast majority of which are uninhabited, provide near ideal conditions for illicit smuggling. Smugglers readily blend in among the armada of pleasure craft traveling throughout the Bahamas archipelago. Recent law enforcement information points to increased smuggling through air traffic, both by newly established commercial traffic from South and Central America and through private planes.

Cuba

The native Amerindian population of Cuba began to decline after the European discovery of the island by Christopher Columbus in 1492 and following its development as a Spanish colony during the next several centuries. Large numbers of African slaves were imported to work the coffee and sugar plantations, and Havana became the launching point for the annual treasure fleets bound for Spain from Mexico and Peru. US intervention during the Spanish-American War in 1898 assisted the Cubans in overthrowing Spanish rule, with full independence being obtained in 1902, after which the island experienced a string of governments mostly dominated by the military and corrupt politicians. Fidel Castro led a rebel army to victory in 1959 and he ruled for nearly five decades, despite extensive US Sanctions. For more details see Part 1 Section 3, Sanctions & Embargoes above. Fidel stepped down as President in February 2008 in favour of his younger brother Raúl Castro. Cuba's Communist revolution, with Soviet support, was exported throughout Latin America and Africa during the 1960s, 1970s, and 1980s. Cuba is criticised by many for close relationships with Venezuela, Iran and North Korea, co-ordinating policies and resources in a partnership aimed at counteracting and circumventing US Foreign policies.

Numerous serious allegations have been made against the Cuban regime, including: i) the development and testing of electromagnetic weapons that have the capacity to disrupt telecommunication networks, cut power supplies and damage sophisticated computers; ii) the export of biotechnology to Iran; iii) contacts with designated terrorist groups, including Hamas and Hezbollah, the Popular Front for the Liberation of Palestine, IRA and ETA; iv) providing a safe haven for fugitives particular from US justice and v) weapons supply deliveries to North Korea.

The latest case involved the detection of 2 Cuban MiG-21 jet fighters found aboard a seized North Korean cargo ship in the summer of 2013, intercepted by Panamanian authorities off the Atlantic entrance to the Panama Canal on a 508-foot North Korean freighter Chong Chon Gang. Officials searching the vessel found the MiG aircraft in sealed containers hidden under 100-pound bags of sugar – 10,000 tons worth – in the ship's hold. They also uncovered 15 jet engines and other weaponry. The UN has imposed an embargo on arms shipments to North Korea stemming from that country's 2006, 2009 and 2013 nuclear tests.

Cuban territorial waters and air space serve as a transhipment zone for US and European bound drugs. Cuba is a source country for adults and some children subjected to forced labour and sex trafficking. Prostitution of children reportedly occurs in Cuba as prostitution is not criminalised for anyone above 16 years old.

Dominican Republic

The Dominican Republic shares this Caribbean island with Haiti, and prior to its independence in 1844 was known as Santo Domingo and before that as part of Hispaniola, from which Haiti also emerged after being discovered by Christopher Columbus on his first voyage in 1492. Mostly non-representative rule followed, and in the last half of the twentieth century, Joaquín Balaguer maintained a tight grip on power for the next 30 years until 1996. Since then former President Leonel Fernández Reyna (first term 1996-2000) won election to a new term in 2004 following a constitutional amendment allowing presidents to serve more than one term, and was since reelected to a second consecutive term.

The Dominican Republic is a transhipment point for South American drugs destined for the US and Europe and has become a transhipment point for ecstasy from the Netherlands and Belgium destined for US and Canada. It is also a suspected of being used for money laundering in particular by Colombian narcotics traffickers. As far as Human Trafficking is concerned, Haitian migrants cross the porous border into the Dominican Republic to find work and illegal migrants from the Dominican Republic cross into Puerto Rico.

Jamaica



Jamaican organised crime is a powerful force in Jamaica and a significant part of the criminal world in the cities of the US, Canada and the UK and Canada. The major crime groups are deeply involved in the international drug trade and within Jamaican protection rackets and extortion. They have

penetrated the formal economy in both legitimate and illegitimate businesses. They have massive political influence with corruption endemic.

Yardies/Posses - Shower Posse - Jamaica

The posses or Yardies are loose groupings of gangs that first became involved in drugs and gun-running in the early 1980s and have been described by some as an example of organised disorganized criminals. Many authoritative studies have claimed that the Jamaican posses are closely linked to Jamaican political parties including the Jamaica Labour Party and the Peoples National Party. This political control extends to the ability to deliver votes and communities with JLP posses controlling the south and west of Kingston whilst the PNP posses control central and eastern. Few Posses claim to have no political allegiance. In the UK Jamaican criminal gang members are often referred to as Yardies. Hurricane Charlie devastated Jamaica in 1951 and the government set up the Hurricane Housing Organisation which created social housing projects with very basic amenities. In this poverty crime and violence flourished. The term Yardie stemmed from the slang name, originally used pejoratively, to occupants of "government yards", and was used affectionately by newly arrived Jamaican immigrants to Britain and then by extension to Jamaican gangs in London. As Jamaica entered the 1980s, the island found itself being exploited as a trans-shipment point for cocaine and the criminal gangs exploited this opportunity. In order to benefit further and follow the drugs, Jamaican criminals chose foreign city areas that already contained large populations of lawful Jamaicans to establish their foreign operations and gain more control over the drugs being trafficked, for example, London and New York, New Jersey, Florida, and Pennsylvania.

One of the first and most infamous of the Posses is the 'Shower Posse'. There are differing reports on the origin of the name. One theory is that it comes from the promises of its associated politicians to shower supporters with gifts. Another view is that it is a reference to the gang showering opponents with bullets. The Shower Posse's home is in Tivoli Gardens in Jamaica, which is also the district of ex-Jamaica Labour Party, PM Bruce Golding (2007-2011).

In the 1980s the Shower Posse were believed to have formed branches in sixteen major American cities including Miami and New York, and in Toronto, Australia and Italy. The leader of the Shower Posse at its height was Christopher Coke also known as Dudus took over his father's gang, becoming the leader of Kingston's Tivoli Gardens, distributing money to the area's poor, creating employment and setting up community centres while also exporting vast quantities of marijuana and cocaine. Coke had a privileged upbringing, being sent to school with children of the country's political elite. He is reputed to have made billions of US\$ before his arrest in Jamaica in 2010 after an extradition request from the US was received in 2009 and pressure was applied to enforce it.

In 1989, Shower Posse member Charles "Little Nut" Miller was arrested in the US, charged with drug trafficking and obtaining immunity identified Christopher Coke as the leader of the gang back in Jamaica and a man with close ties to the Jamaica Labour Party. At the time of his 2010 capture Jamaican police were unable to enter this neighborhood without community consent. In a run-up to Coke's arrest, more than 70 people—security forces and civilians died in a 2010 raid of the Kingston neighborhood he was associated with. He was picked up at a Jamaican checkpoint disguised in female clothing. He was eventually extradited to New York, where he would face charges and be convicted of smuggling drugs and weapons in June 2012.

Haiti

Formerly Hispaniola and discovered by Christopher Columbus in 1492, run by the Spanish then the French, Haiti became the first post-colonial black-led nation in the world, after a slave revolt, declaring its independence in 1804. Currently the poorest country in the Western Hemisphere, through corrupt leaders such as Papa doc Duvalier and then his son Bebe doc Duvalier and more recently President Aristide until his ejection in 2004, and still recovering from a 2010 devastating earthquake (the worst in 200 years in the region) which was estimated to have killed over 300,000 and left some 1.5 million homeless. Haiti is a source, transit, and destination country for men, women, and children subjected to forced labour and sex trafficking with many of Haiti's trafficking cases involving children recruited to live with families in other towns in the hope of going to school but who instead become forced domestic servants known as restaveks who are vulnerable to abuse and make up a large proportion of Haiti's population of street children, who are forced into prostitution, begging, and street crime by violent gangs; Haitians are exploited in forced labour in the Dominican Republic, elsewhere in the Caribbean, and the US. Haiti is also a Caribbean transhipment point for cocaine en route to the US and Europe.

Central America



Central America consists of the seven states of Belize, Honduras, Guatemala, Costa Rica, Nicaragua, and El Salvador with a combined area smaller than Texas.

The Central America Four Agreement between El Salvador, Guatemala, Honduras, and Nicaragua allows for free movement of the citizens of these countries across their respective borders without passing through immigration or customs inspection, although for all practical purposes the whole of Central America has unrestricted movement.

Costa Rica and Panama are much better off and better governed than their neighbours. Costa Rica is one of the world's oldest democracies; life expectancy there is on a par with the US. The others have suffered diffident economic growth in the past decade. Nicaragua is the poorest country in mainland Latin America. Almost half of Guatemala's children are chronically malnourished, a rate worse than Ethiopia's, and said by the World Bank to be the third-worst in the world. Political conflict compounded these problems. The civil wars that ravaged Central America in the 1970s and 1980s between dictators backed by the US and guerrillas backed by the Soviet Union and Cuba are over, but a crippling polarisation of right and left remains.

In 2010 the Inter American Commission on Human Rights reported that Latin America had had the highest levels of youth violence in the world being 36 times that of developed countries. Spain's population roughly equates to that of Central America yet in 2006 it had 336 murders whilst Central America had over 14000. For every murder there are approximately 40 crimes of non-fatal violence. Today organised drug crime has increased its already substantial presence and widened its activities. It is now the main cause of the bloodshed within Central America which is used as a bridge between Colombia and Mexico and from there onwards to the US.

These problems are even more acute in the so called Northern Triangle of Guatemala, El Salvador and Honduras.

Northern Triangle

Honduras, Guatemala and El Salvador make up the so-called Northern Triangle of Central America with each fighting for survival caught between the rise in

criminal violence domestically and the presence of the international drug trade. A bleak economic landscape has fostered youth gangs known as maras and domestic smugglers to build a relationship with the great drug syndicates of Mexico and South America with impunity permitted by a corrupt police and government.

In the past decade criminality has risen exponentially throughout Central America, but the crime wave has overwhelmingly been felt much more strongly in the Northern Triangle. Guatemala's rate of 46 murders per 100,000 people is more than twice as high as Mexico's, and nearly ten times greater than that of the US. Honduras and El Salvador are more violent still. Nicaragua, Costa Rica and Panama, the quietest members of the group, have also seen violence increase in recent years, as has Belize

Honduras, El Salvador and Guatemala's security forces are in a standoff with transnational drug cartels trying to control territory to use as transportation routes for drug trafficking. The drugs, mostly cocaine, are produced in South America and smuggled through the three countries to the US. The trade is managed by powerful Mexican cartels, especially the Sinaloa, and using local gangs as support and muscle. The three countries are also increasingly becoming drug producers and processing sites. They register some of the highest homicide rates in the world.

According to some commentators, including Douglas Farah, the countries of the Northern Triangle, particularly Honduras could be labeled "narco" or "failed" states.³³ In 2011, a Costa Rican non-governmental organisation (NGO) concluded that several Central American nations were at risk of becoming "failed states".³⁴ In 2011, a Costa Rican non-governmental organisation (NGO) concluded that several Central American nations were at risk of becoming "failed states" with Honduras labeled the most at risk, and with governments losing the ability to tackle their security problems leaving large sections of "ungoverned spaces" where criminal operations effectively control the territory. For example, the Petan, a sprawling, sparsely populated jungle region in northern Guatemala, has become a landing zone for clandestine flights from Colombia and Venezuela. In the Laguna del Tigre national park lies a "cemetery" of more than 30 crashed light aircraft which had been used to ferry cocaine. Locals are paid by narcos to keep the runways open.

The road to this state of affairs is at once complex and simple. Extreme poverty, massive inequality and virtually non-existent infrastructure in many areas coupled with state institutions that are riddled with corruption form a receptive breeding ground for the various groups involved in the movement of cocaine from the Andean states to Mexico and its ultimate destination the US. Added to this, individuals involved in the conflicts of the 70s and 80s have no employment and possess weapons superior to those held by the police.

Indigenous gangs have existed for decades moving

drugs, contraband, humans and arms but now the Mexican Cartels have moved in as drug flights from South America into Mexico become more difficult and seaborne interdiction more effective on the Caribbean and Pacific routes into Mexico and the US.

So called 'Go Fast' boats can land at myriad safe coastal areas and flights can land in territories that are controlled by the smugglers. Small aircraft are often crash landed as they are seen as 'disposable'. Most of the organisations that participate in drug-trafficking in the Northern Triangle are tasked primarily with the protection and transportation of Colombian or Mexican owned products. One example of this relationship is the Mexican Sinaloa Cartel's links with Los Perrones Orientales, an organised crime group that transports product by land from the Pacific Coast to Guatemala.

Somewhere between 250 and 350 tonnes of cocaine or almost the whole amount heading for the US now pass through Guatemala each year, according to American officials. Whereas a decade ago Central America seized less cocaine than either Mexico or the Caribbean, in 2008 it intercepted three times more than the other two combined. Mexico's Sinaloa, Gulf and Los Zetas Cartel's are now active through much of the isthmus, often with local allies. Unlike the Colombians, they pay their local help in drugs, not cash.

The impact has been lethal. Guatemala's murder rate has doubled in the past decade. In both Guatemala and El Salvador, the rate of killing is higher now than during their civil wars. Guatemala's government reckons that about two-fifths of murders are linked to the drugs business. Even Panama, much richer than many Central American countries and a favourite retirement spot for wealthy foreigners, has seen its murder rate almost double in the past three years. As well as using Central America as a corridor, the traffickers are moving more of their operations there.

Another part of the organised crime structures are youth gangs. There is evidence that the upper echelons of transnational youth gangs, such as the Mara Salvatrucha (MS13), provides security, or "muscle," for the Mexican cartels and frequently provide transport services for organisations like Los Perrones Orientales. These upper levels are often made up of former combatants from former conflicts in the region.

The other main Mexican cartel is Los Zetas and there is evidence that they have recruited senior Mara 18 members. They also recruit from the notorious disbanded Guatemalan Special Forces known as the Kabilas.

Mara 18 is the local name of the 18th Street Gang that originated in Los Angeles in the US and came to the region when gang members were deported from the US back to Central America. There are an estimated 70,000 maras in Central America. These youth gangs are a ready supply of willing teenagers who can ferry drugs, look

after kidnap victims and carry out other low-level crimes although they run large scale protection racket.

Mexico's cartels, which are the most powerful in Latin America were initially Transportistas for the Colombians but eventually wrested control from them. The maras of Central America, have close ties to inner-city gangs in the US and it is feared may well be seeking to emulate the Mexican's cartels experience.

Belize is similar in many respects with regard to drugs, whilst smuggling of persons is more developed with both human smuggling and trafficking taking place. Large Belizan communities exist in New York and Los Angeles and gangs such as the Bloods and the Crips from Los Angeles are to be found in Belize. Honduras recently had a coup and as a consequence organised crime has spread and escalated. Insofar as the Cartels and gangs are concerned for all practical purposes they operate in a transnational environment so nation states and national institutions are of little concern.

Costa Rica is a more stable democracy yet the effects and influence of the Mexican cartels is growing. Recent successes have seen the arrest of some of the Michoacana crime family, infamous for its use of torture by what they call Divine Justice.

Mara - MS13/MS18 - Central America

The smuggling clans of Central America (known as *transportistas*) and the larger transnational elements in Mexico and the Andean drug producer Countries hire Maras to perform smaller scale criminal such as drug running, targeted murders and extortion. Generally speaking, Maras are violent criminal organisations that began as turf gangs who originally engaged in local opportunistic criminal activities, but have now internationalized into networked and complex structures with a growing political consciousness. Maras are functionally different from the native criminal groups found elsewhere in the Americas and are now the quintessential Central American criminal link in the transnationalised Latin American drug trade network. The maras phenomenon finds its origin on the streets of the poor and racially segregated neighborhoods of 1960s Los Angeles. The first recognisable Mara to take shape was the 18th Street gang comprised of Mexican and Central American immigrants. The original Maras were formed by Latino workers who were shunned by the established American gangs that existed in the immigrant areas of the city (around the 18th street); namely the Chicano (or Mexican-Americans) and African-American gangs. At first in order to defend themselves from the dominant gangs, the migrants banded together but with time they ended up adopting the profile of an inner city American gang eventually growing to a powerful force in their own right and now known as the Mara Salvatrucha (or MS13), slang for Salvadoran mob. The MS13 benefited from experiences in El Salvador's brutal civil war which gave them an advantage and established the MS13 as a major force of violence. Though at one

point the Maras were all relegated to the slums of east LA, they were soon exported to other parts of the US once other illegal Central American immigrants joined the gangs in other diaspora communities throughout the country, most notably those of Chicago and New York City. The gangs' swelling ranks also coincided with the first waves of deportation initiated by US after ending of the Central American civil wars in the early 1990s. The criminally radicalized immigrants were returned in droves to their countries taking with them the Mara culture. In the case of the Northern Triangle states, no others have been as significant as the 18th Street and MS13. The continuous deportation of illegal immigrants essentially seeded gang members from the US to the Northern Triangle, thus bringing with them their vicious rivalries, unique marero ethos and the gangs' organisational makeup. The Maras' expansion in the past two decades is astonishing. It is estimated that nearly 70,000 mareros exist in Central America alone, with an equal high number living in the US. Honduras is accountable for over half at 36,000, while Guatemala has 14,000 and El Salvador has 10,400 mareros. The nearest count in any neighboring country is 2,660 in Costa Rica. Honduras has the dubious distinction of having the most number of different gangs in Central America with over 100 different maras vying for control, while El Salvador and Guatemala are almost neatly split between the feuding MS18 and MS13.

El Salvador

The archbishop of San Salvador, Óscar Romero, had been an outspoken critic of the ruling military junta attempting to quell a popular insurrection whose leaders were advocating social and economic reforms. Romero alleged that the junta was guilty of massacres and torture. The archbishop was assassinated on 24 March 1980. Rallies in support of Romero turned bloody when police opened fire on the crowds. This was the spark for the 12-year El Salvador civil war. The military, supported by the US, targeted union officials, clergy, academics and others; thousands died. A peace agreement was reached between the two groups in 1992.

People's Liberation Forces (El Salvador) - El Salvador
The People's Liberation Forces (FPL) was one of the first Salvadoran terrorist groups to emerge in the 1970s, formed by then secretary general of the Communist Party of El Salvador (PCES). It was hoped that a violent struggle led by FPL insurgents could bring about a popular revolution and thus led El Salvador into an era of Communism. The group also strongly opposed foreign investment, and as is to be expected of a left-wing political group, detested perceived US 'imperialism'.

During the 1970s the FPL represented the largest terrorist groups operating in El Salvador. In particular the tendency of grassroots political activists to work within the political system, rather than attempt to cripple it through military action, proved highly divisive. In

1980 the FPL merged with **Farabundo Martí National Liberation Front (FMLN)**, a similarly leftist terrorist group through which it continued its resistance to El Salvador's government.

Farabundo Martí National Liberation Front (FMLN) - El Salvador

The Farabundo Martí National Liberation Front (FMLN) was a Marxist-Leninist insurgency movement operationally active in El Salvador from 1980 to 1992. The organisation was founded in 1980 as the unification of five left-wing political groups in El Salvador and aimed to overthrow the contemporary government. In terms of structure the organisation was delineated between a political wing that focussed on the group's propaganda campaigns, and a military wing that conducted violent insurgency.

Considerable financial aid was provided by other Communist regimes and affiliated "solidarity" groups distributed throughout Latin America, Europe and North America. Revenue was also sourced from "taxes", typically levied from businesses located in contested areas of El Salvador, as well as kidnappings and bank robberies.

Military training was provided for many FMLN members by Nicaragua and Cuba. In 1982 the FMLN commenced two offensives against El Salvador's government, however both were defeated by the state's military. Despite these setbacks, by 1983 the FMLN is believed to have reached the height of its power and commanded as many as 12,000 insurgents. Supplied with American weapons purchased by Nicaragua and Cuba the FMLN launched its final conventional military campaign against El Salvador's government in 1983. However, having failed to secure a decisive victory by means of open warfare, in the latter half of the 1980s the FMLN moved away from open warfare in favour of urban guerrilla tactics. Rather than large units organised along tradition military lines the group restructured itself to operate in smaller cells and engaged in bombings, arson, and kidnappings. Most notable among these kidnappings was the FMLN's seizure of President Jose Napoleon Duarte's eldest daughter Inez in 1985.

As well as government facilities, American interests and citizens became high priority targets in reaction to the US's provision of aid to the government of El Salvador and its counterinsurgency operations. For instance in 1985 4 US Marine security guards were gunned down at a road side cafe, and in 1987 the driver of the US Navy Attache was kidnapped and killed. Such attacks continued until in 1991 a peace settlement was reached between the FMLN and the El Salvadorian government. Since then the FMLN has turned away from political violence, participating successfully in El Salvador's political arena.

Today the FMLN is one of the two largest political parties in El Salvador and in 2009 won the Presidential election with its candidate Mauricio Funes.

Honduras

Once part of Spain's vast empire in the New World, Honduras became an independent nation in 1821. When compared to other Central American countries, Honduras suffered fairly low levels of political violence and terrorism in the second half of the 20th century. Full-scale leftist insurrections did not materialize in Honduras as they did in Guatemala and El Salvador, and, consequently, neither did the rightist paramilitary groups that combated them. The 1980s, however, saw an increase in political violence in the country, though not to the levels of its neighbors. A few leftist groups did emerge, such as the Morazanist Patriotic Front, but their attacks remained few in number and small in scope.

Honduras is a transshipment point for drugs and narcotics, and suffers from corruption which is considered a major problem. Honduras is a source and transit country for men, women, and children subjected to sex trafficking and forced labour. Honduran women and girls, and, to a lesser extent, women and girls from neighboring countries, are forced into prostitution in urban and tourist centers; Honduran women and girls are also exploited in sex trafficking in other countries in the region, including Mexico, Guatemala, El Salvador, and the US.

Guatemala

Guatemala endured a long and bloody conflict between government and leftwing rebels. Its roots date back to the mid-40s when the US helped overthrow the October Revolutionaries, leftwing students and professionals advancing radical social and economic reforms. The CIA-backed a coup in 1954 and the military junta put an end to the left wing reforming agenda. In the 80s, the junta aimed to systematically eliminate leftwing activists throughout civil society, the universities, politics, law, peasants, etc. More than 200,000 people were killed over the course of the 36-year-long civil war that began in 1960 and ended with peace accords in 1996. About 83% of those killed were Mayan, according to a 1999 report written by the UN-backed Commission for Historical Clarification titled "Guatemala: Memory of Silence." The report also concluded that the vast majority, 93%, of human rights violations perpetrated during the conflict were carried out by state forces and military groups. US involvement in the country was also singled out by the commission as a key factor contributing to human rights violations, including training of officers in counterinsurgency techniques and assisting the national intelligence apparatus.

Peace accords ending the 36-year internal conflict were signed in December of 1996. Today Guatemala is led by President Álvaro Colom of the National Unity for Hope. Almost 15 years after the end of the civil war, violence and intimidation continue to be a major

problem in political and civilian life. Organised crime groups operate with relative impunity, an issue that appears likely to factor prominently in the country's next presidential election later this year.

Panama

In Central America, Panama is the most developed economically. Though it lies in Central America, the country's 3.6 million citizens are now richer than most Latin Americans. Whilst Panama's economy outclasses others in Central America, and many in South America, its government is in turmoil. Ricardo Martinelli, a supermarket tycoon who became president in 2009, is at war with his vice-president, Juan Carlos Varela, who comes from a different party and whom the constitution prevents the president from sacking. Mr Varela has accused the president of taking a US\$30mio bribe in return for awarding a contract for helicopter and radar services to an Italian firm. Mr Martinelli is suing Mr Varela for US\$30mio in damages. A leaked cable from the US embassy reveals that in 2009 Mr Martinelli requested help in the wiretapping of his political opponents, noting his "penchant for bullying and blackmail."

Panama was once part of Colombia until it seceded in 1903 with the backing of the US who then went on to start building the critically strategic (to the US) Panama Canal in 1904.

A cursory glance at a map shows how its geographic location along with its developed maritime and transportation infrastructure facilitates the trans-shipment of illegal drugs from the Andean producers to the US and Europe.

Traffickers exploit these advantages which include five containerised seaports, the Pan-American Highway and an international hub airport. Further there are many uncontrolled airfields, and a Pacific and Atlantic coastline which is virtually unguarded. Smuggling of weapons and drugs particularly between the isolated Darien region and Colombia has gone on for over a century but boats and planes form the main modes of transport.

In the hinterland hundreds of abandoned or unmonitored legal airstrips are used by traffickers for refuelling or deliveries. Panama was for a time considered by many a Narco-state, where drug cartels from Colombia in particular were given licence to operate transhipment of drugs north, particularly under the Presidency of [General Manuel Noriega](#) until his removal by US forces in 1989. Panama today is an important regional financial centre and has a sophisticated international banking sector. Its de facto currency is the US dollar. Panama also has the Colon Free Zone (CFZ) which is the world's second largest free zone after Hong Kong.³⁴

Nicaragua

In 1979, the Sandinista National Liberation Front overthrew Anastasio Somoza's dictatorship in July and established a socialist coalition government. The Somoza family had ruled Nicaragua from 1936 to 1979, allegedly embezzling funds on a massive scale, including monies sent to help rebuild the capital, Managua, after an earthquake in 1972. This led to the establishment of rightwing rebel groups formed in opposition to the Sandinistas, who would become known as the [Contras](#) and who received aid from the US government, for arms and training, until aid was outlawed by Congress.

The US administration of Ronald Reagan, which had come to power in 1981 committed to supporting rightwing regimes in Latin America and attempted to fund the groups covertly, with the Contras-Sandinista conflict seen by many as a proxy for the cold war. For more details also see [Arnoldo Aleman](#) in Part 2 Section 7 below.

Nicaraguan Democratic Force-(Contra's) - Nicaragua
The Nicaraguan Democratic Force (FDN) was established in 1981 from many members of the deposed Somoza government's National Guard and others. The Sandinista government had risen to power in 1979.

The US supplied the group with considerable support and provided a safe haven for the political wing of the organisation, which established its headquarters in Miami, Florida.

The FDN was the largest Contra Group (the label given to all rebel groups violently opposing the Sandinista government) operating in Nicaragua. A rare glimpse into the financial dealings of the rebel group was provided by the testimony of FDN leader Adolfo Calero before a Federal grand jury in 1987. In the documents revealed to the court it was clear that Saudi Arabian sources provided vast sums of money to support the FDN.

The group also used complex commercial organisations to act as dummy institutes and secret bank accounts to channel money to their cause. For instance a friend of Calero's employed in the legal profession granted the FDN leader access to a bank account in Miami that belonged to one of his family members. Into this account monthly instalments were paid by FDN patrons. Mr Calero's friend also helped to spin the web of commercial deceit still further by setting up three dummy companies based in Panama which held five bank accounts in Panama and the Cayman Islands. Through these bank accounts the FDN channelled further funds without attracting the attention of law enforcement agencies.

It also emerged that in 1986 the FDN had received

large sums of money from the US despite a Congressional ban on the provision of aid. Moreover that money had itself been raised by the secret and illegal sale of weapons to Iran in what came to be known as the Iran-Contra affair.

The contra campaign against the Sandinista government ended when the left wing party was voted out of office in 1990 national elections, a development that also spelt the end of FDN military action.

Belize

Belize was the site of several Mayan city states until their decline at the end of the first millennium A.D. The British and Spanish disputed the region in the 17th and 18th centuries. It formally became the colony of British Honduras in 1854. Territorial disputes between the UK and Guatemala delayed the independence of Belize until 1981.

Current concerns include, high crime rates, the country's growing involvement in the Mexican and South American drug trade, with Belize becoming a transshipment point for cocaine, a small-scale illicit producer of cannabis, primarily for local consumption and the presence of an offshore finance sector where concerns around money laundering activity related to narcotics trafficking and other crimes exist.

Costa Rica

Although explored by the Spanish early in the 16th century, it wasn't until 1563 that a permanent Spanish settlement was established and the area remained a colony for some two and a half centuries. In 1821, Costa Rica became one of several Central American provinces that jointly declared their independence from Spain. Two years later it joined the United Provinces of Central America, but this federation disintegrated in 1838, at which time Costa Rica proclaimed its sovereignty and independence. Since the late 19th century, only two brief periods of violence have marred the country's democratic development.

Costa Rica is a transshipment country for cocaine and heroin from South America, it produces cannabis in remote areas and has concerns over domestic cocaine consumption, particularly crack cocaine. Of particular note are seizures of smuggled cash in Costa Rica and at the main border crossing to enter Costa Rica from Nicaragua.

South America



The South American continent, vast and geographically diverse stretches from the Northern Hemisphere through Equatorial jungles and down to the sub-Antarctic polar climate of Tierra del Fuego. Thirteen countries share (predominantly) two similar languages,

Spanish and Portuguese; one principal religion and a common historical background. Historically South America has in one way or another lived under the political shadow of its northern neighbour (the US). Today however, whilst the US still has much influence several factors are changing the political landscape away from real or perceived US dominance.

It is 40 years since the death of Chilean President Salvador Allende, who died in the presidential palace on 11 September 1973 during a coup led by army chief Augusto Pinochet. Allende won the presidency in 1970 and became Latin America's first democratically elected leftwing leader. Pinochet instituted Operation Condor through the 1970s and 1980s which amounted to a campaign of political repression carried out by US-backed Latin American dictatorships that was designed to eliminate tens of thousands of leftwing activists. Whilst it was the idea of Pinochet, he enlisted Argentina, Bolivia, Paraguay, Uruguay and Brazil in a continent-wide campaign. Today South America looks very different with a BBC report in 2005 estimating that, of 350 million Latin Americans, three out of four lived under leftwing administrations. Hugo Chávez was among the first of the late 20th-century Latin American leaders who came to power with a leftwing agenda. Chávez looked to Simón Bolívar, godfather of South American independence, for inspiration for his Latin socialism. He was elected president of Venezuela in 1999 and served until his death earlier this year. Elected president of Brazil in 2002 and re-elected in 2006, the former union leader Luiz Inácio Lula da Silva promised major social reforms and oversaw the emergence of Brazil as an economic powerhouse, which did much to raise millions of people in the country out of poverty. Tabaré Vázquez, an oncologist, was elected president of Uruguay in October 2004. A member of the Socialist party, he became the country's first president from a leftwing party. One of his first actions was to announce a US\$000mio-a-year project to alleviate extreme poverty. Michelle Bachelet's election as president of Chile in 2006 was significant for a number of reasons. She was the first woman president, she was a social democrat, and her father, General Alberto Bachelet, who served under Allende, had been tortured by, and died during, the Pinochet dictatorship.

Evo Morales, elected President of Bolivia in 2006, is a champion of indigenous rights and a vocal critic of US foreign policy. He has committed himself to help the poorest peasant farmers and to ensuring that the wealth from the country's gas reserves is distributed more equally. Rafael Correa, elected in 2006 as President of Ecuador and re-elected for a second term. He is an economist who came to power on the back of his opposition to the International Monetary Fund's plans for remedying his country's economic ills. Instead, he rolled back the IMF plans and put an end to privatisation of national resources such as water, oil and gas.

The Tri-Border Region

The tri-border region, formed by the cities of Puerto Iguazu, Argentina, Foz do Iguaçu Brazil and Ciudad del Este, Paraguay, has a reputation for lawlessness and an historical presence of terrorist elements. For decades the region has been home to various smugglers, terrorists, drug traffickers, arms dealers, and organised crime figures from Russia, Japan, China, and Nigeria, among other countries. Terrorists from the Middle East have also been found in the area, particularly from Lebanon and Syria. Former FBI director Louis Freeh described the area as a "free zone for significant criminal activity, including people who are organised to commit acts of terrorism." Approximately 630,000 people live in the tri-border area, of which roughly 25,000 are Arabs or of Arab descent. The dynamics of the area, including political corruption and lax border security make it a haven for crime helping to fuel a huge underground economy and even, according to some commentators, links to terrorism and the financing of terrorism. In particular, US officials have voiced concerns about the tri-border area, arguing that its history of being a home to terrorists and fugitives, as well as rampant corruption, make it an ideal location in which subversive groups can operate, for example Islamist terrorists. The Islamist terrorist element in the tri-border region dates back to 1992, when a car bomb exploded at the Israeli Embassy in Buenos Aires, killing 29 people and injuring more than 200 and 2 years later, in July 1994, the Argentine-Israeli Mutual Association (AMIA) Jewish Center was bombed, killing 86 people. The investigations eventually implicated Hezbollah, Argentine authorities believe that the attacks were organised and planned in the tri-border area. Others claim Al-Qaeda are linked to the bombings as the two bombings have similarities to the US Embassy bombings in Kenya and Tanzania, which were carried out by Al-Qaeda. Francis X. Taylor, the US State Department's coordinator for counterterrorism, noted in testimony to the US Congress that the tri-border region had a "long-standing presence of Islamic extremist organisations." While he did not mention Al-Qaeda, he did name Hezbollah and al Gammaa al-Islamiya specifically as being involved in "fundraising activities and proselytising among the large expatriate population from the Middle East."

Brazil



South America's biggest country and of a similar size to the US with a population of over 190 million, is Brazil, which today boasts the world's seventh largest economy. Brazil was officially "discovered" in 1500, when a fleet commanded by Portuguese diplomat Pedro Álvares Cabral, on

its way to India, landed in Porto Seguro, between Salvador and Rio de Janeiro. Following three centuries under the rule of Portugal, Brazil became an independent nation in 1822 and a republic in 1889. By far the largest and most populous country in South America, and of a similar size to the US with a population of over 190 million, Brazil overcame more than half a century of military intervention in the governance of the country when in 1985 the military regime peacefully ceded power to civilian rulers. Brazil's first colonizers were met by Tupinamba Indians, one group in the vast array of the continent's native population. Lisbon's early goals were simple: monopolise the lucrative trade of pau-brasil, the red wood (valued for making dye) that gave the colony its name, and establish permanent settlements. Brazil has ten neighbouring countries giving about 10,000 miles of land borders and nearly 4,600 miles of Atlantic coastline. Half of the land borders are with Bolivia, Peru and Colombia, major cocaine-producers.

These geographical factors alone make it inevitable that Brazil is a transit country for narcotics traffic to Europe, Africa and to a lesser degree, the US. Brazil also has an increasing domestic consumption drug problem and is a likely probable source of precursor chemicals for cocaine processing. Cocaine enters Brazil via land, river and by small aircraft from Colombia, Peru and Bolivia on its way to mainly Africa and Europe. Brazil's international airports are commonly used as departure points for couriers carrying drugs on or in their person, in their baggage, or as hold cargo. The northeast coast of Brazil is the closest transatlantic shipping point to West Africa and well within the easy reach of a range of vessels enabling its seaports to ship drugs in containers and other ships. The same routes are used in reverse to bring Ecstasy and amphetamines back to Brazil. This is also a route for much precursor chemical products although many of the precursor chemicals are readily available within Brazil and it is known that traffickers are moving their labs across the border from Bolivia to obtain easier precursors. Increasing cocaine paste seizures in Brazil also suggest that raw Bolivian cocaine is increasingly being refined in Brazil. Internally Brazil has been increasing its attempts to control those 'favelas'

controlled by gangs that have for some time become untouchable centres for criminality. In a raid in the Vila Cruzeiro and Alemao favelas a special task force seized 300 kilograms of cocaine and 42 metric tonnes of marijuana. 350 stolen vehicles were recovered as well as 518 weapons, including grenades, machine-guns, and bazookas. Money laundering in Brazil is mainly linked to domestic crime, such as drug trafficking, public and private corruption, organised crime, gambling and a thriving smuggling trade in many types of contraband. Concern remains about significant illicit financial activity in the Tri-Border Area.

As the administration of President Dilma Rousseff struggles to follow the success of former President Luiz Inácio Lula da Silva, particularly in trying to reverse the trend of declining rates of economic growth, she had to face continued questions on corruption with the largest political corruption trial in the country's history, which recently concluded with guilty verdicts for 25 of the 37 people indicted and questions around the forthcoming 2014 World Cup and 2016 Olympics likely to increase as these events get closer. Known as the mensalão corruption scandal, this party financing corruption case has been at the centre of Brazilian politics for a decade and has shone a light to the heart of the political system leading to sentences for José Dirceu, the chief of staff and closest political adviser to former Brazilian president Luiz Inácio Lula da Silva during his first administration (2003–2006), to nearly 10 years in jail. At the same time, the court convicted 25 other co-conspirators in Dirceu's scheme, which involved bribing congressmen to vote in lockstep with the government, and also implicated banks, advertising agencies, and politicians. The court estimated that the scheme involved the embezzlement of at least US\$150m in public funds. At first, Lula tried to stay aloof from the trial, maintaining that he had been "betrayed" by the defendants and that he "knew nothing" about the scheme. When he was sentenced to more than 40 years in jail, Marcos Valério, an advertising executive and a principal in the scheme, told prosecutors that Lula had personally authorised him to borrow money from banks so that the funds could be used to buy off members of congress. In light of these revelations Brazil's chief public prosecutor announced that he had ordered a formal investigation of Lula's role in the scheme. Allegations of corruption against Brazil's top politicians is not unusual, for example see the case of Paulo Maluf in Part 2 Section 7 below.

Blue Command - Brazil

Calling themselves 'militias' they are also known as the Blue Command and are created mainly by retired police, some active police, prison officers and firemen. Until recently they occupied 92 favelas in Rio and levied charges on the inhabitants for 'protection' and restricted freedom of movement. Incredibly the Blue Command charged the inhabitants for gas, the use of TV channels and several other services.

Red Command - Brazil

Comando Vermelho or Red Command is a major Brazilian criminal organisation engaged primarily in arms and drug trafficking. The group was formed in 1979 when a collection of ordinary convicts and left-wing political prisoners were incarcerated together during the military dictatorship of 1964-1985 and formed Falange Vermelha (Red Phalanx). In the early 1980s the group changed its name to the Comando Vermelho and is said to have lost its political ideology. The Comando Vermelho controls parts of Rio de Janeiro and has fought several small-scale conflicts (in 2001 and 2004) with the rival gang Terceiro Comando which itself emerged out of a power struggle amongst the leaders of Comando Vermelho during the mid-1980s. The organisation is a collection of independent cells rather than having a strict hierarchy, however prominent bosses include Luiz Fernando da Costa, Isaías da Costa Rodrigues. In late June 2007, Rio de Janeiro police launched a large-scale assault on the area where up to 24 people were killed. According to a study by Rio de Janeiro University's Violence Research Center, in 2008 the group controlled 38.8% of the city's most violent areas, down from 53% in 2005. The Comando is particularly associated with a popular Brazilian musical style, called funk. Funk artists are also sponsored by the Comando Vermelho to record songs that promote the group and eulogize the group's dead members, which sell well via Radio and street vendors in Rio de Janeiro and in São Paulo.

First Capital Command (PCC) - Brazil

In São Paulo a group that dominates the massively overcrowded prisons but is also a significant threat outside is called The PCC,³⁵ with at least 6,000 senior leaders and over 140,000 members. (The First Command of the Capital: after its Portuguese initials). Also known as Primeiro Comando da Capital (PCC), the gang began in 1993 at a football match in Taubaté Penitentiary, São Paulo, amongst a group seeking to avenge the victims of 1992's Carandiru Massacre. This massacre, during which numerous atrocities were allegedly perpetrated, witnessed the death of more than a hundred prisoners by the São Paulo military police in a vicious backlash against prison riots. The PCC was founded on a sixteen point manifesto that outlines the organisation's ideology, as well as its code of conduct. Chief among the aims laid out in the manifesto is the goal to fight injustice and oppression in the Brazilian prison system, purportedly seeking "Liberty, Justice, and Peace" in its place. One might imagine these rather lofty ideals for an organised crime syndicate; however the PCC code of conduct contained in the manifesto also bears traces of an ethical orientation somewhat unusual for a prison gang. For instance members of the PCC are prohibited from mugging, rape, extortion, or the use of the gang's framework to settle personal conflicts. However the PCC is in truth far from a wholly law abiding body, maintaining close ties with the

drug trafficking organisation Red Command. Though part of the financial revenue generated from this illicit trade may be used to pay some gang members through law school, such criminal enterprise demonstrates the willingness of the group to transgress ethical and legal boundaries in the pursuit of expansion. Moreover the expansionist ambitions harboured by the PCC set their sights far beyond prison walls, perceiving itself as a potent political force with the ability to "revolutionize Brazil from within prisons". As an organisation the PCC is supported by a strict hierarchical structure, whereby members pay monthly subscriptions and fulfil designated roles as 'soldiers', 'towers' or 'pilots'. 'Soldiers' act as the organisation's rank and file 'muscle', while 'towers' fulfil leadership duties in their particular prison, and 'pilots' coordinate communications between groups. In 2001 the PCC demonstrated the strength of this network by coordinating rebellions in twenty-nine prisons across the state of São Paulo. Since 2002 the gang has been led by Marco Willians Herbas Camacho, a man also known by the title Marcola or 'Playboy'. Amongst prisoners Camacho is regarded as somewhat of an intellectual and has risen to iconic status in the eyes of many Brazilians.

Argentina

In 1816, the United Provinces of the Rio Plata declared their independence from Spain. After Bolivia, Paraguay, and Uruguay went their separate ways, the area that remained became Argentina and is the second largest country in South America. Argentina gets its name from the Spanish word 'argentino'. The word literally translates to silver. The country's population and culture were heavily shaped by immigrants from throughout Europe, with Italy and Spain providing the largest numbers. Up until about the mid-20th century, much of Argentina's history was dominated by periods of internal political conflict between Federalists and Unitarians and between civilian and military factions. After World War II, an era of Peronist populism and direct and indirect military interference in subsequent governments was followed by a military junta that took power in 1976. Democracy returned in 1983 after a failed bid to seize the Falkland Islands (Islas Malvinas) by force, and has persisted despite numerous challenges, the most formidable of which was a severe economic crisis in 2001-02 that led to violent public protests and the successive resignations of several presidents. Allegations against the current government of Argentina's President Cristina Fernández de Kirchner as well as against herself are increasing. In one case, an emissary from Hugo Chavez, then president of Venezuela, was discovered at Buenos Aires airport carrying a briefcase full with US\$800,000 in cash. Whilst Kirchner denied the allegation, there were claims made that the money was to support Kirchner's presidential bid. Within

Argentina, many question the huge fortune Kirchner and her late husband Nestor amassed since taking public office. Her declared personal wealth stands at US\$13.8mio, up from US\$500,000 when the couple first entered national politics. Kirchner cites income from real estate and hotels the couple had purchased to explain the 2,600% return on the couple's investments. In its foreign relations, Argentina, has antagonized traditional allies such as Brazil, Spain and the US, while growing ever closer to Iran, Venezuela and Cuba. Argentina has become a major transit route for Bolivian and Peruvian cocaine headed to West Africa and then onward to Europe. The President's son, Máximo Kirchner, leads a group of young presidential advisers and government officials known as "La Cámpora," who believe they are the vanguard of a transformational generation that will help Argentina regain its rightful place as a world leader. The Camporista take their name from Héctor José Cámpora, an ally of the late dictator Juan Perón and of the armed radical left wing of Peronist movement that became the Montonero guerrillas. Cámpora served as president for 49 days in 1973, just long enough to sign an amnesty to allow Perón, then living in exile, to return and run for President.

People's Revolutionary Army - Argentina

The People's Revolutionary Army of Argentina terrorized the Argentine government and foreign corporations from 1960 until 1977 when it was effectively eradicated by the Argentine Military. The People's Revolutionary Army, or ERP, was founded as the armed wing of the communist political organisation, the Workers Revolutionary Army Argentina. ERP's principal goal was to overthrow Argentina's military-ruled government. In large part due to its success the Argentine government granted the military expanded powers to eradicate terrorist elements, principally the ERP, thus beginning in 1975, the Argentine military's "dirty war," with mass disappearances and hit squads employed. The ERP had financed itself through bank robberies, kidnapping and extortion.

Anti-Communist Alliance - Argentina

The Argentine Anti-Communist Alliance was a right-wing, semi-official terrorist group active during the mid-1970s. The Peronist government, led by Isabel Perón, the wife of former dictator Juan Domingo Perón, secretly created the Triple A in 1974 to terrorize radical left-wing groups responsible for hundreds of assassinations of police and military officials. The group was famous for assassinations, bombings, and torture. From 1974-1976, the Triple A waged war on Argentina's political left under the leadership of José López Rega, the Minister of Social Welfare and a long-time advisor to the Perons. The war between leftist terrorists and the Triple A grew out of a split between supporters of Juan Domingo Perón. Perón had attracted rabid support from both the left and the right. Leftists saw him as a populist who would bring about socialist revolution, while the right-wing supported his economic and political nationalism. When Perón was restored to power

after a seventeen-year absence in 1973, he publicly cast aside his far-left built better relationship with the church and economic elites. The left-wing of the Peronist movement, referred to as the Montoneros, became outcasts and took up arms. The violence escalated until military leaders staged a coup on March 24th 1976 to restore order. The leaders of the coup dissolved the Triple A in mid-1976. The army then took over the group's "counter-terrorism" responsibilities. What followed was a massive campaign of state terror against suspected subversives that resulted in as many as 30,000 deaths. This period, which lasted until 1983, is referred to as "the dirty war." The new military leaders used many of the same techniques, personnel, and even cars used by the Triple A. Thus, the Triple A is often described as the precursor to the state terror of the dirty war.

Paraguay

Paraguay achieved independence from Spain in 1811. Paraguay lost and gained territory in numerous wars with its neighbours. Paraguay, despite an increase in political infighting, has held relatively free and regular presidential elections since its return to democracy in 1989. This following the 35-year military dictatorship of Alfredo Stroessner. The current President, elected in 2013, is also the leader of the Party that Stroessner led, the Colorado Party. Horacio Cartes, whose term runs through to 2018, built a family fortune with two dozen companies under Grupo Cartes that dominate industries from banking to tobacco to soft drinks to soccer. The corruption watchdog group Transparency International ranks Paraguay 150th worst out of 176 countries. Paraguay is a major illicit producer of cannabis and a transshipment country for Andean cocaine headed for Brazil, other South American markets, and Europe. Paraguay contributes through weak border controls to concerns in the Tri-Border Area.

Uruguay

Uruguay once claimed by Argentina declared its independence from Brazil in 1825 and secured its freedom in 1828 after a three-year struggle. Its capital, Montevideo was founded by the Spanish in 1726 as a military stronghold, but with a natural harbour it soon became an important commercial center. Whilst strong civilian governments ruled throughout much of the twentieth century a violent Marxist urban guerrilla movement named the Tupamaros, launched in the late 1960s, led Uruguay's then president to cede control of the government to the military in 1973. By year end, the rebels had been crushed, but the military continued to expand its hold over the government, with civilian rule civilian rule being restored only in 1985. In 2004, the left-of-center Frente Amplio Coalition won national elections that effectively ended 170 years of political control previously held by the Colorado and Blanco parties. Uruguay is a source country for women and children

subjected to sex trafficking and, to a lesser extent, a destination country for men, women, and children exploited in forced labour; most victims are women and girls exploited in sex trafficking. Uruguay is a small-scale transit country for drugs mainly bound for Europe, often through sea-borne containers; law enforcement corruption; money laundering because of strict banking secrecy laws; weak border control along Brazilian frontier; increasing consumption of cocaine base and synthetic drugs.

Tupamaros - Uruguay

The Tupamaros were a group of urban guerrillas who operated in Uruguay (primarily Montevideo) from early 1960s to the 1980s. At one time, there may have been as many as 5,000 Tupamaros operating in Uruguay. Although initially they saw bloodshed as a last resort to achieving their aim of improved social justice, their methods became increasingly violent as the military government cracked down on citizens. In the mid-1980s, democracy returned to Uruguay and the Tupamaro movement laid down their weapons in favour of joining the political process. They are also known as the MLN (Movimiento de Liberación Nacional, National Liberation Movement) and their current political party is known as the MPP (Movimiento de Participación Popular, or Popular Participation Movement). In early-1960s, the Tupamaros committed a series of low-level crimes such as robberies, often distributing part of the money to Uruguay's poor. The name Tupamaro is derived from Túpac Amaru, last of the ruling members of the royal Inca line, who was executed by the Spanish in 1572. It was first associated with the group in 1964.

Ecuador

The "Republic of the Equator" was one of three countries that emerged from the collapse of Gran Colombia in 1830 (the others are Colombia and Venezuela). Although Ecuador marked 25 years of civilian government in 2004, the period has been marred by political instability. Seven presidents have governed Ecuador since 1996. Ecuador's President Rafael Correa, a US-educated economics professor whose father spent time in an American jail for smuggling cocaine, has long cast himself as a US adversary, and last year put his anti-American rhetoric to the test by allowing WikiLeaks founder Julian Assange to take refuge at Ecuador's embassy in London and considered an asylum request by the former National Security Agency contractor and self-described whistleblower Edward Snowden who is evading charges under the US Espionage Act.

Ecuador is inevitably affected by neighboring organised illegal drugs operations in Colombia which penetrate across Ecuador's shared border and as a result Ecuador

is a significant transit country for cocaine originating in Colombia and Peru. It is an importer of precursor chemicals used in production of illicit narcotics as well as an attractive location for cash-placement by drug traffickers laundering money because of the dollarisation of the Ecuadorian economy and a relatively weak anti-money laundering regime. Allegations have been made that Ecuador have benefited from funds generated by the sale of cocaine from the Revolutionary Armed Forces of Colombia (FARC) and that senior members of the government have supported the FARC. Further negative allegations around corruption, particularly in the judiciary, and accusations against those close to the President as well as governmental attacks against the media cause significant concerns. After decades as a transit route for cocaine and a secondary money laundering center, Ecuador is emerging as a key meeting ground for multiple transnational criminal and terrorist organisations and an important part of a pipeline that moves not only cocaine but human cargo, weapons, precursor chemicals and hundreds of millions of dollars a year.

Bolivia

Bolivia is named after independence fighter Simon Bolivar who broke away from Spanish rule in 1825. Much of its subsequent history has consisted of a series of nearly 200 coups and countercoups. Democratic civilian rule was established in 1982, but leaders have faced difficult problems of deep-seated poverty, social unrest, and illegal drug production. In December 2005, Bolivians elected Movement Toward Socialism leader Evo Morales president, by the widest margin of any leader since the restoration of civilian rule in 1982, after he ran on a promise to change the country's traditional political class and empower the nation's poor, indigenous majority. However, since taking office, his controversial strategies have exacerbated racial and economic tensions between the Amerindian populations of the Andean west and the non-indigenous communities of the eastern lowlands. In December 2009, President Morales easily won reelection, and his party took control of the legislative branch of the government, which will allow him to continue his process of change. Bolivia is the world's third-largest cultivator of coca (after Colombia and Peru) and the third largest producer of cocaine, estimated at 195 metric tons potential pure cocaine in 2009, a 70% increase over 2006. Bolivia is a transit country for Peruvian and Colombian cocaine destined for Brazil, Argentina, Chile, Paraguay, and Europe. Whilst Bolivia has had numerous terrorist groups operating in the Country over the past 30 years, these are now inactive

or cease to exist. They included the National Liberation Army (Bolivia).

National Liberation Army - Bolivia

The National Liberation Army (ELN) was founded by Ernesto "Che" Guevara. Following his participation in Cuba's 1959 communist revolution, Guevara left for Bolivia in late 1966, where he spearheaded the National Liberation Army. Within a year, Guevara was captured by US-trained Bolivian security forces and in 1967, a day after his capture, Che Guevara was executed. NLA continued its insurgency into the early 1970s but it was not successful and the ELN was eliminated. Between 1990 and 1993, a new terrorist organisation, the Nestor Paz Zamora Commission emerged claiming to be a reconstituted NLA, however this has been disputed.

Chile

It is 40 years since the death of Chilean President Salvador Allende, who died in the presidential palace on 11 September 1973 during a coup led by army chief Augusto Pinochet. Allende won the presidency in 1970 and became Latin America's first democratically elected leftwing leader. The CIA, which played an active part in Chilean politics in the 1970s, sought Allende's overthrow before he took office in 1970, but the US disputes that it was involved in the military coup. Operation Condor though was put in place through the 1970s and 1980s amounting to a campaign of political repression carried out by US-backed Latin American dictatorships that was designed to eliminate tens of thousands of leftwing activists. It was the idea of Chilean dictator Augusto Pinochet, who enlisted Argentina, Bolivia, Paraguay, Uruguay and Brazil in a continent-wide campaign.

Movement of the Revolutionary Left (MIR) - Chile

The Movement of the Revolutionary Left (MIR) was a Chilean terrorist organisation active from the mid-1960s through the mid-1990s. The group was originally formed in 1965 by left leaning students at the University of Concepcion who had broken away from the Socialist Party. In 1967 the group began to undertake bank raids in order to finance itself and some members travelled to Cuba to receive military training. The MIR also pledged its alignment with the individual form of socialism espoused by Fidel Castro in Cuba, a move that resulted in the provision of financial aid by the Cuban state. During the Frei presidency, when the Chilean government was formed by the Christian Democratic Party, the MIR refused to participate in the electoral process, instead engaging in urban guerrilla warfare against the state. Even when a coalition of Chilean socialist and communist parties known as Unidad Popular (UP) came together and was elected to government in 1970,

the MIR persisted in remaining outside of the political process. Later the MIR offered what it described as 'critical support' to the UP party, arguing that while Allende's reforms certainly represented progress, they did not go far enough. During the overthrow of the Allende government the MIR engaged in military resistance and continued to do so throughout the Pinochet regime. At this time the MIR also cemented its links with other militant leftist groups operating in Latin America, forging an alliance with the Tupamaros, Peoples' Revolutionary Army in Argentina and the National Liberation Army operating in Bolivia. This unified group was known as the JCR or Junta Coordinadora Revolucionaria. Nevertheless, despite building up a sophisticated organisational network that included international links and significant military capabilities, the MIR's strength was considerably weakened by a crackdown from Pinochet's government that led to the arrest and death of many senior MIR leaders. Later, in the 1980s the MIR began to place greater onus on political action, though it continued to embark on intermittent spates of violent protest. Today the MIR exists solely as a political organisation, albeit a relatively small one, that peacefully contests votes within the Chilean political system.

Manuel Rodriguez Patriotic Front (FPMR) - Chile

In 1983, the Chilean Communist Party established an armed wing known as the Manuel Rodriguez Front or FPMR (Frente Patriotico Manuel Rodriguez) to violently oppose the Chilean government. The organisation intended to lead an armed struggle that would see the government of Augusto Pinochet deposed and bring about a revolution in Chilean society. In particular the group hoped it could spark a mass uprising through daring attacks that would publicise its movement, as well as demonstrate the vulnerability of the dictatorship to violent protest. One such attack was launched in September 1986 when the FPMR attacked a motorcade in which Pinochet was travelling. The assassination attempt was ultimately unsuccessful, however 5 of Pinochet's guards were killed, demonstrating just how close the militants came to achieving their goal. In truth such attacks did not in fact inspire popular rebellion, but rather isolated the Communist Party and the FPMR, and unified the more moderate opposition groups. At the height of its power the FPMR was estimated to have between 500 and 1,000 members and is known to have received financial support from Cuba. However, following the fall of the Pinochet regime the organisation experienced a period of fracture. With the return of democracy to Chile many FPMR members advocated returning their campaign for a Communist state to legal methods within the political system, while more radical militants preferred to continue the armed struggle. This latter faction was responsible in 1991 for the assassination of the right wing Chilean senator Jaime Guzman, as well as the kidnapping of Cristian Edwards del Rio, son of the owner of Chilean newspaper El Mercurio. After being held hostage for 145 days del Rio was released by the militant FPMR faction when his family handed over US\$1mio in ransom to his captors. In 1996 the

dissident FPMR faction also succeeded in an audacious operation to free four of its members from a high security prison in Chile. The plan involved hijacking a tourist helicopter, from which a rope was lowered into the prison for the captive members to ascend. Despite shots from prison officers all four members successfully escaped in the helicopter, which then landed in Santiago where cars waited to complete the getaway. Today the group is no longer active and therefore poses no terrorist threat.

Peru

Peru was the seat of several prominent Andean civilizations, most notably that of the Incas who were descended from one of the oldest civilizations in the world, known as the Norte Chico, whose empire was captured by Spanish conquistadors in 1533, who established a Viceroyalty, which included most of its South American Colonies. Peruvian independence was declared in 1821, and remaining Spanish forces were defeated in 1824. After a dozen years of military rule, Peru returned to democratic leadership in 1980, but experienced economic problems and the growth of a violent insurgency, with both the [Shining Path](#) and the [Tupac Amaru Revolutionary Movement \(MRTA\)](#). President [Alberto Fujimori](#)'s election in 1990 ushered in a decade that saw a dramatic turnaround in the economy and significant progress in curtailing guerrilla activity. Nevertheless, the president's increasing reliance on authoritarian measures, masterminded by his intelligence chief, [Vladimir Montesinos](#) and an economic slump in the late 1990s generated mounting dissatisfaction with his regime, which led to his ouster in 2000. A caretaker government oversaw new elections in the spring of 2001, which installed Alejandro Toledo as the new head of government, Peru's first democratically elected president of indigenous Quechuan ethnicity. The presidential election of 2006 saw the return of Alan Garcia who, after a disappointing presidential term from 1985 to 1990, oversaw a robust economic rebound. In June 2011, former army officer Ollanta Humala was elected president, defeating Keiko Fujimora Higuchi, the daughter of [Alberto Fujimori](#). Peru was until 1996 the world's largest coca leaf producer. Peru is now the world's second largest producer of coca leaf, though it lags far behind Colombia.³⁶ Cocaine is moved to Brazil, Chile, Argentina, and Bolivia for use in the South America and shipped out from Pacific ports to the international drug market.

Shining Path - Peru

In the 1960s, Sendero Luminoso, otherwise known as Shining Path, grew out of the Communist movement in Peru. Shining Path's Luminoso's radical Marxist

ideology was shaped by its founder and long-time leader, Abimael Guzman Reynoso. Abimael Guzman, a former university professor, was able to use his position within academia to gain credibility and entice students to his fledgling Communist movement. In fact, for a decade and a half, Shining Path primarily waged a war of militant Maoist ideas and propaganda. It was not until May 1980 that Shining Path turned to violence as a means of transforming a 'bourgeois democracy' into what Guzman described as 'New Democracy' (an idea derived from a Maoist principle stipulating that a society could move into socialism without first enduring a period of capitalist rule).

Once the Shining Path turned to violence, the group unleashed a brutal terrorist campaign within Peru, responsible for the deaths of many Peruvian citizens. The imagery with which Shining Path announced the initiation of its violent campaign against the government institutions of Peru and any perceived counter-revolutionaries is also worthy of note. In a gruesome spectacle members of Shining Path killed dogs in the Peruvian capital of Lima and suspended them from traffic lights and lampposts, affixed next to the slogan "Deng Xiaoping, Son of a Bitch" (Deng Xiaoping served as 'paramount leader' of the People's Republic of China 1978-1992, and was perceived to be a counter-revolutionary by Shining Path. Shining Path's stated goal is nothing short of an entire re-ordering of Peruvian society and institutions, a supposedly defunct structure that would be replaced by Communist institutions. At first the organisation was dismissed as marginal and at odds with the mainstream left in Peru, a political block that had returned to participation in electoral politics following the end of military rule and the return to democracy in 1980. The group also appeared out of sync with Peru's larger political trajectory, with many of Shining Path's socialist principles having already been realised some years prior to the organisation's inception. For instance the government redistributed 8.6 million hectares to more than 370,000 families between 1968 and 1975, rendering part of Shining Path's social revolution already complete. By the mid-1980s Shining Path was becoming increasingly hard to ignore, as was the organisation's embrace of violent tactics in its campaign. Violence was not, however, confined to Shining Path militants, but was also perpetrated on a large scale by the Peruvian military, which saw in the conflict an opportunity to quell both Shining Path terrorists and any other groups with the potential to subvert government authority. The leader of this crackdown, President Alberto Fujimori, is today serving a prison sentence for his part in government corruption and the administration of death squads. For more details see Part 2, Section 7, Criminal Cases for both [Alberto](#)

Fujimori and Vladimiro Montesinos.

Despite the rise of centre-leftist coalitions to power in 1983 and 1985 Shining Path maintained its commitment to a revolutionary war, seizing control of large swathes of the countryside and conducting deadly attacks across Peru. The most prominent of such attacks came in 1983 when 69 men, women, and children were brutally massacred in the town of Lucanamarca. Another notable attack occurred in 1992 when the detonation of two car bombs in the Miraflores district of the Lima resulted in the death of 20 people, along with the injury of 250 others. In 1992 Shining Path's leader Abimael Guzman was arrested and has remained in prison serving a life sentence. This development, alongside significant counter-insurgency operations by the Peruvian government, has led to the sharp decline of the organisation. Nonetheless, while undoubtedly a depleted force, Shining Path continues to operate and in 2012 killed more than a dozen Peruvian security personnel. The organisation's political wing, Movadef, also showed signs of revival in September 2012. It is believed that Shining Path and Movadef members have established themselves within some labour organisations, using these groups as both a political cover and a source of recruitment. The group is also believed to be closely involved with the drug trafficking industry, deriving much of its funding from this source.

Tupac Amaru Revolutionary Movement (MRTA) - Peru

The Tupac Amaru Revolutionary Movement (MRTA) is a Peruvian based group that sought to overthrow the national government during the 1890s. The organisation grounded its ideology in Marxist-Leninist revolutionary theory and intended to establish a democratic socialist state in place of the existing 'bourgeois' democracy. MRTA's second goal was to eradicate the commercial and diplomatic influences of the US and other foreign nations in Peru. Formed by Victor Polay Campos in 1984, the group derived its name from the 18th century rebel leader Tupac Amaru, who became a martyr after leading an unsuccessful rebellion against Spanish colonial rule. The name was also thought to appeal to Peru's rural population, a key group amongst whom the MRTA sought to garner appeal. The organisation also attempted to forge strong links with industrial workers (particularly those belonging to trade unions) and Peruvian students. In terms of military strength the MRTA could not challenge its rival Peruvian guerrilla organisation Shining Path, numbering at its height only 600 active militants. The enmity between these two groups was considerable, with Shining Path forcing the MRTA out of some of Peru's main drug producing region and hence depriving it of a valuable source of

revenue. Ideologically the two groups also stood apart, with MRTA's leadership perceiving Shining Path as excessively fundamentalist in its approach to socialism and levelled accusations of Stalinism at its left wing challenger. The MRTA's anti-state military campaign began in 1986, undertaking ambushes, kidnappings, bombings and assassinations. Among the most noteworthy of the MRTA's military accomplishments was the capture of the provincial capital of Juanji, which militants successfully held against state forces for several months in 1987. The organisation was dealt a considerable blow in 1992 however with the arrest of leader Polay Campos. Nevertheless operations continued in Campos' absence and in 1996 MRTA staged its most famous attack. On 17 December 1996 MRTA militants occupied the Japanese Ambassadorial residence in the Peruvian capital of Lima, seizing hostage hundreds of diplomats and government officials who were attending a function to celebrate the Emperor's 63rd birthday. Most of the hostages were released soon after the initial raid, however others were held captive for 126 days. Eventually all but one of these final hostages were freed by Peruvian military forces; the one hostage fatality occurring during the operation to free the prisoners. All 14 of the MRTA militants inside the Ambassadorial residence died, along with 2 Peruvian commandos. Since the infamous 1997 hostage taking the MRTA has not been implicated in any other significant terrorist attacks and the organisation has been deemed inactive.

Colombia



Colombia was one of the three countries that emerged from the collapse of Gran Colombia in 1830 (the others are Ecuador and Venezuela). Colombia was formerly known as New Granada, within Gran Colombia. To the west of Venezuela lies the Republic of

Colombia, named after the man who "discovered" the Americas. Today the name epitomises drug cartels and decades long terrorist/insurgent struggles.

Preconceptions aside it is the fourth largest country in South America with substantial oil reserves whilst being a major producer of coal, gold, silver, emeralds, platinum. Sadly, it has also been ravaged by a long violent conflict that has gone on for decades involving outlawed armed groups, drug cartels and gross violations of human rights. Things have improved since 2002 although there are still many deep rooted social problems. For nearly five-decades a long conflict between government forces and anti-government insurgent groups, principally the Revolutionary Armed Forces of Colombia (FARC) heavily funded by the drug trade, escalated during the 1990s. More than 31,000 former paramilitaries had demobilised by the end of 2006 and the United Self Defense Forces of Colombia (AUC) as a formal organisation had ceased to function. In the wake of the paramilitary demobilization, emerging criminal groups arose, whose members include some former paramilitaries. The insurgents lack the military or popular support necessary to overthrow the government, but continue attacks against civilians. Large areas of the countryside are under guerrilla influence or are contested by security forces.

In October 2012, the Colombian Government started formal peace negotiations with the FARC aimed at reaching a definitive bilateral ceasefire and incorporating demobilized FARC members into mainstream society and politics. The Colombian Government has stepped up efforts to reassert government control throughout the country, and now has a presence in every one of its administrative departments. Despite decades of internal conflict and drug related security challenges, Colombia maintains relatively strong democratic institutions characterized by peaceful, transparent elections and the protection of civil liberties.

Colombia is a massive illicit producer of coca, opium poppy and cannabis being the world's leading coca cultivator with 116,000 hectares in coca cultivation in 2009, producing a potential of 270 mt of pure cocaine; is the world's largest producer of coca derivatives; supplies cocaine to nearly all of the US market and the great majority of other international drug markets. Of course, Colombia is home to drug trafficking organisations that are successors to the famous Cali Cartel's and the operation of Pablo Escobar and perhaps not as well known they remain highly successful and profitable working with other groups, particular with Mexican Drug Trafficking Organisations and partners to supply and profit from drug production and supply. A significant portion of narcotics proceeds are either laundered or invested in Colombia through the black market peso exchange.

April 19 Movement (M-19) - Colombia

The April 19 Movement (M-19) emerged following the narrow defeat of Rojas Pinilla in the Colombian presidential election of 1970. Former dictator Pinilla ran as a member of the National Popular Alliance Party (ANAPO) and despite receiving substantial support from the urban working classes only managed to command enough votes to secure second place. While the majority of ANAPO purportedly accepted the outcome and condemned the use of violence, a splinter group seceded from the mainstream party and formed M-19. This group distinguished itself from the other main terrorist organisations operating in Colombia (namely FARC and ELN) in that it followed a more general left-wing ideology centred on helping the nation's poor, rather than a Marxist-Leninist or even Maoist ideology championing a complete socialist revolution. Irrespective of ideological motivations, M-19 began a campaign of violence that lasted for two decades. In 1990 this fighting finally came to a close with M-19 agreeing to a ceasefire and turning solely to politics under the new title of the Democratic Alliance M-19.

United Self-Defence Forces of Colombia (AUC)

The AUC was an umbrella organisation of death squads, some of them formed in the 1980s, focused on two goals: fighting leftist guerrillas and making money, most of it from drug trafficking. In 2003, the AUC agreed to enter negotiations with the government. In return for dismantling their forces and aiding criminal investigations, the top AUC leadership was promised a certain degree of amnesty. The demobilisation, however, proved to be a false peace. Most paramilitary blocs only handed in a small fraction of their weapons.

Special Focus 16 FARC / The Revolutionary Armed Forces of Colombia - Colombia



The FARC, represents one of Latin America's oldest, largest, and best-equipped insurgencies. It began in the early sixties as an outgrowth of Colombia's peasant self-defence leagues that later adopted Marxist-Leninist ideology. FARC's central aim is to overthrow Colombia's

government and enact socialist reforms, but central among the demands of the peasant orientated organisation is a redistribution of land. Estimates of land ownership currently concentrate 52% of Colombia's total arable land in the hands of 1.5% of the country's landowners, an imbalance that is perceived by many among the agricultural poor as a great social injustice.

In terms of organisation structure FARC is governed by a general secretariat led by co-founder Antonio Marin (a.k.a. Manuel Marulanda or "Tirofijo") and six others, including senior military commander Victor Suarez (a.k.a. Jorge Briceno or "Mono Jojoy"). The group is organised along military lines and includes some specialized urban fighting units. FARC has been responsible for bombings, murders, mortar attacks, kidnappings, extortion, and hijacking, as well as guerrilla and conventional military action against political, military, and economic targets associated with the Colombian government. Internationals have also fallen victim to FARC attacks, for instance in February of 2003, following the crash-landing of a US plane in a FARC-held area, the group murdered a US citizen and a Colombian, and continues to hold hostage the three other US citizens onboard. US citizens have been particularly targeted by FARC operations as a consequence of both the organisation's loathing of what it sees as American imperialism, and the provision of US aid for the counterrevolutionary operations of the Colombian government. This support came in the guise of an anti-drug smuggling policy, however in truth the Clinton administration provided funds to the Colombian government primarily for the purposes of fighting the FARC insurgency and the communist

threat that the US associated with the group. In a confidential memorandum discovered in 1996 US Ambassador Myle Frechette even admitted that FARC's initial reputation for drug trafficking "was put together by the Colombian military, who considered it a way to obtain US assistance in the counterinsurgency". Since then the original fiction has become a reality and FARC does indeed have considerable involvement in the Colombian drugs trade. Returning however to the US hostages taken by FARC in 2003, with 5 years having passed the Colombian government granted Venezuelan President Hugo Chavez permission to negotiate with FARC to secure the release of the three US citizens and 42 other so-called "political" hostages, some held as long as a decade. Colombia ended Chavez's role after he repeatedly disregarded Colombian positions; however, FARC did release two hostages. The kidnapping of foreign citizens has also continued, with FARC using the ransoms to fund its military campaigns.

Today FARC has well-documented ties to the full range of narcotics trafficking activities, including taxation, cultivation, and distribution, all of which it uses to finance continuing operations. As of January 2013 peace talks between the Colombian government and FARC continue, though reports have thus far been largely positive. Issues under discussion include land reforms, the illegal drugs trade, political participation, disarmament and reparation payments for victims of the conflict. Chief among the proposals offered by FARC is that 25 million hectares of land (approximately 25% of Colombian land) be given to the nation's poor. FARC has also requested that the Colombian government legalize the cultivation of some crops used in the production of illegal drugs, such as cocoa, poppies and marijuana.

ELN / National Liberation Army - Colombia

The ELN is a Cuban Revolution-inspired group, heavily influenced by the early actions and theories of Fidel Castro and Che Guevara. The ELN emerged following the overthrow of the Cuban government by Guevara and Castro in 1959. The National Liberation Army was founded by two distinct groups. The first group comprised of urban, left-wing intellectuals with strong ties to rural farmers. They co-founded the group with a radicalized group of oil sector unionists from Barrancabermeja's oil industry. Radical members of the Catholic clergy joined the group in late 1965. This was the first time that Christians and Marxists had joined together in a Colombian revolutionary movement. The ELN's unique founding philosophy strongly emphasized socialism, mixing Castro-ism with the liberation theology of the Catholic Church. More concretely, the ELN's self-appointed role was

to represent the rural poor and decrease the foreign presence in Colombia. The ELN's goal was to take power from the Colombian government and replace it with a more egalitarian "popular democracy" that would represent all Colombians equally under the law. The ELN strongly opposed foreign investment, in part due to its location in an oil-rich area and its connections to trade unionists in the energy sector. The Colombian Department of Administrative Security estimates that in 1998 alone, the ELN obtained US\$84mio from ransoms and US\$255mio from extortion. Employees of oil companies constitute a large percentage of the ELN's targets. The kidnapping and extortion of oil company employees is ELN's primary source of income. This is a natural legacy of ELN's formation in an area rich with oil wells and oil companies. A third, more recent source of income is the collection of a "property" tax from coca and poppy cultivators. It is not known whether the collection of property taxes is a centralized or decentralized activity. Throughout its history, the National Liberation Army steadily gravitated towards violence and armed struggle as a means to attain a socialist Colombia. At the ELN's 1996 national conference, the group decided to decrease emphasis on creating a purely socialist Colombia. Instead, the ELN has returned to its founding objective: popular democracy for all Colombians, propagated at the local level. The ELN has not given up the use of violence in its efforts. The ELN engages in kidnappings, hijackings, bombings, drug trafficking, and extortion activities. It has minimal conventional military capabilities. The group conducts kidnappings for ransom, often targeting foreign employees of large corporations, especially in the petroleum industry. Recently ELN leadership discussed the possibility of ending kidnapping as a means of financing insurgent operations as a government-proposed precondition for formal peace talks. However, the organisation has yet to renounce kidnapping. ELN derives some revenue from taxation of the illegal narcotics industry, and its involvement may be increasing. It attacks energy infrastructure and has inflicted major damage on oil and natural gas pipelines and the electrical distribution network, but has lost much of its capacity to carry out these types of attacks in recent years. Approximately 3,000 armed combatants and an unknown number of active supporters.

ERPAC - Colombia

The Popular Revolutionary Anti-Terrorist Army of Colombia (Ejercito Revolucionario Popular Antiterrorista Colombiano - ERPAC) began as a right-wing proxy of the Colombian government battling leftist guerrillas. Following a failed peace process, the group began doing business with the rebels and other former paramilitaries, controlling vast territory that it

used to process and store cocaine. The ERPAC officially surrendered to the government in 2011, under leader "Caracho," but fewer than half of its members handed in their weapons, leaving the rest to carry on fighting in Colombia's eastern plains. ERPAC's stronghold was in the Meta, Guaviare, Vichada and Casanare provinces of the eastern plains. It controlled production of base and processed cocaine, which it sold to middlemen or exported through networks in Venezuela and Brazil. Since the 2011 surrender, the remnants of the group are thought to have divided into two rival factions, the Libertadores del Vichada, led by Martin Farfan, alias "Pijarbey," who was Cuchillo's second-in-command; and the Meta Bloc, led by Rubber Antonio Navarro Caicedo, alias "Flaco Fredy." Flaco Fredy was captured in 2012, and it is considered possible that Pijarbey will reunite the two groups, perhaps under the command of powerful criminal network the Urabeños.

The Aguilas Negras, or Black Eagles - Colombia

The Aguilas Negras, or Black Eagles, emerged from the so called demobilisation of the United Self-Defence Forces of Colombia (AUC). At times, Aguilas Negras was the generic term used by the government to describe the many fragments of ex-paramilitaries without common leadership committing serious crimes across Colombia. Often, the paramilitary successors who have continued drug trafficking extortion and violence have done so using the Aguilas Negras name. This political bent, along with their lack of a central leadership, distinguishes them in part from the other criminal bands operating in Colombia. Groups using the Aguilas Negras name have since appeared in at least 20 of Colombia's 32 departments, including Nariño, Cauca, Casanare, Guajira, Magdalena, Bolívar, Northern Santander, Santander, Bolívar, Sucre and Córdoba. But the groups appear to operate independently from one another, answering to no central command. Instead, each Aguilas Negras cell concentrates on protecting their small fiefdom and vying with rivals like the Urabeños and Los Rastrojos. The Urabeños was itself at one time described as the "Aguilas Negras of Urabá." A 2006 study by Colombian think-tank Indepaz listed 62 paramilitary successor groups that had registered actions across the country, many adopting names derivative of the AUC blocs. It is possible that in some areas of Colombia, low-level street gangs simply adopt the name "Aguilas Negras" to better intimidate victims into paying extortion fees, or abandoning their property. There is little evidence that the Aguilas Negras operate as a systematic organisation. Instead, it appears to be the blanket name for the many successor groups willing to adapt the AUC's tactics and, in many cases, its political discourse.

Special Focus 17 Colombian Drug Cartels



The Colombian Drug Cartels are criminal organisations developed with the primary purpose of promoting and controlling drug trafficking operations. During the 1980s, as demand for cocaine increased, existing Colombian Cartels

expanded and organised into major criminal conglomerates usually headed by one or several kingpins as in the case of the Medellin Cartel led by Pablo Escobar and the North Coast Cartel, led by Alberto Orlandez-Gamboa "Caracol" (the snail) along with federation-style groups such as the Cali Cartel (founded by the Rodríguez Orejuela brothers, Gilberto and Miguel, as well as associate José Santacruz Londoño) and the Norte del Valle Cartel (Founded by Diego León Montoya Sánchez, Wilber Varela and Juan Carlos Ramírez Abadía).

The Colombian Cartels became notorious and the target of Colombian and US Law Enforcement. Leaders in Cali, Gilberto and Miguel Rodríguez Orejuela, and in Medellin, Pablo Escobar would be brought eventually to justice, the former being captured, extradited and imprisoned in the USA in 2006 and the latter through a bullet which would end his life in a shootout with Colombian Police in 1993. It would take longer to take down the "Caracol" but in 2000 he was arrested and later extradited to the USA leading to the collapse of the North Coast Cartel also.

With the collapse of these major Cartels, a new Organisation, Norte del Valle Cartel, became established and inherited much of the drug trafficking operations, though the establishment of a military wing and infighting have produced "Los Rastrojos" as one of the most important drug trafficking groups in Colombia and beyond. Other Cartels albeit not as powerful do exist including the Cartels in Bogota, Caquetá, and Llano, as well as more than 300 additional drug smuggling organisations or 'Cartelitas' (baby cartels).

Other organisations in Colombia are also involved in drug trafficking including paramilitary or terrorist groups which use the provides of drug trafficking to finance their activities. These include the AUC, Black

Eagles, ELN, FARC, ERPAC, Oficina de Envigado, Los Paisas and Los Urabeños. All the groups currently running the country's drug trade are known collectively by the government as "criminal bands," or BACRIMs.

The Cali and Medellin Cartels - Colombia

The Cali Cartel and the Medellin Cartel both became notorious and the target of Colombian and US Law Enforcement. Leaders in Cali, Gilberto and Miguel Rodríguez Orejuela, and in Medellin, Pablo Escobar would be brought eventually to justice (see above), but until then and for over 20 years, these individuals and the Cartels would become the world's biggest and most profitable criminal narcotic organisations. In 1989, for example, Forbes magazine declared Pablo Escobar as the seventh richest man in the world, with an estimated personal fortune of US \$25 billion.

The life and times of Pablo Escobar has been immortalized by both books and films. He started doing whatever he could to make money. He ran a small gang selling contraband cigarettes and fake lottery tickets. By the time he was 20, he was already an accomplished car thief. In the early 1970s, he was a thief and bodyguard, as well as having a side trade in kidnap before entering the drug trade, working for and then succeeding a successful Medellin contraband smuggler.

The idea of the Cartel was pioneered in Medellin and led to great success. A number of Medellin drug traffickers agreed to pool their shipments of drugs being sent abroad and thus avoid the chances of financial ruin if any individual's shipments were seized. This sensible precaution was also taken on elsewhere and led to the establishment of a federation of traffickers not only in Medellin but also in Cali.

In Cali for example, the Cartel was made up of five major but still independent drug trafficking organisations of whom the most well-known were the two brothers: Gilberto and Miguel Rodríguez Orejuela as well as associate José Santacruz Londoño. The Cali Cartel originally began as a ring of kidnappers known as Las Chamas. The profits of kidnapping helped finance the ring's move to drug trafficking, originally beginning in Marijuana and eventually spreading to cocaine. The cartel's estimated revenue would eventually reach an estimated \$7 billion a year.

In Cali, the organisation would though become increasingly integrated with common shared services including units focussing on: Political: responsible for establishing links with governmental and public officials; Military: handling security, internal discipline and the bribery of military or police officials; Narcotics

and trafficking; This had control over manufacture and shipping; Legal: representation for traffickers held by police, overseas representation, including political lobbyists and Financial: money laundering, front businesses and legitimate businesses. Due to the success of the Cali Cartel the financial unit would be required to establish and maintain complex but professional arrangements which required employing professional managers, accountants, lawyers and technical financial and company experts, both in Colombia and abroad.

The advantage it held over other competitors was really in its distribution network which could move hitherto undreamt of amounts of cocaine. The Cali and Medellin Cartels produced most of the Cocaine and they became the largest players in the multi-billion dollar worldwide cocaine industry. The economics were simple: virtually negligible production costs and soaring end use markets. They also realized and entered into joint agreements with Mexican transportation cartels, which gave them access initially to the North American market but also later into Europe and beyond. As the Colombians lost markets to the Mexicans they sought out European markets.

Given its geographic location, Mexico has long been used as a staging and transhipment point for drugs, illegal immigrants and contraband destined for US markets from Mexico, South America and elsewhere. During the 1980s and 1990s, Colombia's drug cartels in Medellin and in Cali joined with Mexican Gangs involved in trafficking heroin and cannabis, already established an infrastructure that stood ready to serve the Colombia-based traffickers. By the mid-1980s, the organisations from Mexico were well established and reliable transporters of Colombian cocaine. At first, the Mexican cartels were paid in cash for their transportation services, but in the late 1980s, the Mexican transport organisations and the Colombian drug traffickers settled on a payment-in-product arrangement. Transporters from Mexico usually were given 35 to 50 % of each cocaine shipment. This arrangement meant that organisations from Mexico became involved in the distribution, as well as the transportation of cocaine, and became formidable traffickers in their own right, transporting not only to the North American market, but also elsewhere around the world. The current escalation in violence in Mexico is probably a result of a number of factors. The priorities of the Mexican government to tackle the drug cartels has certainly increased, and as cartel leaders are arrested or meet their deaths the balance of power between the various Mexican cartels can shift which also generates bloodshed as rivals move in to exploit the power vacuum. Cocaine is the second most popular recreational drug,

behind Marijuana. Cocaine is commonly used in middle to upper class communities. It is also popular amongst college students, as a party drug. Its users span over different ages, races, and professions. In the 1970s and 1980s, the drug became particularly popular in the disco culture as cocaine usage was very common and popular in many discos. The development of "crack" cocaine introduced the substance to a generally poorer inner-city market. The estimated US cocaine market exceeded US\$70bio in street value for the year 2005, generating massive profits for the traffickers. In comparison this exceeds the annual revenues and profits from another coca inspired product, and No 1 global brand, Coca Cola. Coca-Cola once contained an estimated nine milligrams of cocaine per glass. It was initially formulated in 1886 and sold as a medicine at the time due to the belief that carbonated water was good for the health. It was claimed that Coca-Cola cured many diseases, including morphine addiction. In 1903 the final traces of Cocaine were removed.

World annual cocaine consumption stands at around 600 tonnes, with the US consuming around 50% of the total, Europe about 25% of the total, and the rest of the world the remaining 25%. The 2010 UN World Drug Report reported that the North American cocaine market was valued at US\$38 billion in 2008. According to a 2007 United Nations report, Spain is the country with the highest rate of cocaine usage (3.0% of adults in the previous year). Other countries where the usage rate meets or exceeds 1.5% are the US (2.8%), England and Wales (2.4%), Canada (2.3%), Italy (2.1%), Bolivia (1.9%), Chile (1.8%), and Scotland (1.5%).

Cocaine is moved from Colombia and other Andean countries (particularly Bolivia and Peru) and shipped in numerous ways. These include principally by land through Central America into and through Mexico or by air and transported to staging sites in northern Mexico. The cocaine is then broken down into smaller loads for smuggling across the US-Mexico border. The primary cocaine importation points in the US are in Arizona, southern California, southern Florida, and Texas; Typically, land vehicles are driven across the US-Mexico border. Sixty five percent of cocaine enters the US through Mexico, and the vast majority of the rest enters through South Florida, via smuggling routes throughout the Caribbean, in particular via the Bahamas Island chain. The Colombians now often hire traffickers from Mexico or the Dominican Republic to transport the drugs.

The traffickers use a variety of smuggling techniques to transfer their drugs to US markets. These include the commercial shipment of tonnes of cocaine through

the port of Miami as well as airdrops in the Bahamian Islands or off the coast of Puerto Rico, mid-ocean boat-to-boat transfers and then fast speed boats to the Miami area. Lately even submarines are thought now to be used. Unmanned subs are towed underwater so as to avoid any radar profile and if a towing boat is approached it can ditch instantly the sub so that no evidence exists if the towing boat is boarded. Transponders allow later recovery on some.

Cocaine is also carried in small, concealed quantities across the border by couriers known as "mules" (or "mulas"), who cross a border either legally, for example, through a port or airport, or illegally elsewhere. The drugs may be strapped to the waist or legs or hidden in bags, or hidden in the body. If the mule gets through without being caught, the gangs will reap most of the profits. If he or she is caught however, gangs will sever all links and the mule will usually stand trial for trafficking alone.

With massive profits being generated the Cartels faced the problem of how to launder and retain these profits. This was probably not so difficult initially during the 1970s as the Cartels along with other drug traffickers placed their money in offshore financial centres where few questions were asked about the origin of the monies. With growing profits however they needed to consider how to deal with the huge amounts of cash they were generating.

A book released by Pablo's brother, Roberto Escobar, called "The Accountant's Story" told of how at its height the Medellín drug cartel was smuggling 15 tons of cocaine a day, worth more than half a billion dollars, into the US. According to Roberto, his brother's operation spent US\$2,500 a month just purchasing rubber bands to wrap the stacks of cash, and since they had more illegal money than they could deposit in banks, they stored the bricks of cash in their warehouses, annually writing off 10% as "spoilage" when the rats crept in at night and nibbled on the hundred dollar bills.

The traffickers created a large complex network of front companies involved in all areas of business activity, for example: Hundreds of companies were set up in Construction, Retail, Agriculture, Manufacturing, Radio and Television stations, Hotels and Investment Companies. The drug monies would be laundered through these Companies and large profits made by these Companies would be used for further investment in the drugs trade and the rest banked offshore. In addition to front Companies, legitimate companies were also invested in, one for example being a pharmaceutical

chain in Colombia called Drogas la Rebaja which had 400 shops in 28 cities.

Whilst much could be channelled through a variety of front organisations the cartels also used a method known as the Black Market Peso Exchange which also dovertailed neatly into the activities of some of the front companies (see Part 1, Section 1, Smuggling, for details).

Another avenue used to launder funds was the establishment of a Bank, licensed in a jurisdiction with little supervision and either operating as a brass plate or Shell Bank or with a license to conduct only non-domestic business. For example, Gilberto Rodríguez Orejuela became Chairmen of the Board of the Banco de Trabajadores which enabled some amounts to be laundered and later on he founded the First Inter-Americanas Bank in Panama.

It took until 1989 for the G-7 to establish the Financial Action Task Force in Paris which would start to address this problem from a global perspective laying down 40 recommendations for action targeted at Countries in order to attack the proceeds of drug trafficking.

As mentioned in 1993 and following a prolonged manhunt Escobar was shot dead. In 1991 Escobar had given himself up to Colombian Police as the USA had made him public enemy number 1. Extradition was prohibited at this time under Colombian Law. Escobar though continued his criminal activities within Prison, until fearing worse conditions he fashioned an escape. In 1992 US and Colombia together trained and advised a special Colombian police task force, known as the Search Bloc, which had been created to locate Escobar. At the same time, a vigilante group financed by his rivals and former associates, including the Cali Cartel and right-wing paramilitaries would also target him and his Organisation and bring his reign to an end.

As for the Cali Cartel and the Rodriguez Brothers they would last much longer. In 1995 US President Clinton issued Executive Order 12978, "Blocking Assets and Prohibiting Transactions with Significant Narcotics Traffickers," under authority of the International Emergency Economic Powers Act and called upon the US Treasury to target Colombian drug cartels using financial sanctions. Under this authority, OFAC launched the Specially Designated Narcotics Traffickers ("SDNT") programme. The objectives of the SDNT programme were said "to isolate and incapacitate the businesses and agents of the Colombian drug cartels by publicly exposing them, freezing their assets, and denying them access to the financial system and to

the benefits of trade and transactions involving US businesses and individuals. The SDNT list referred to "527 companies and 815 individuals involved in the ownership or management of the 21 Colombian drug cartel leaders' business empires. The businesses named as SDNTs ranged across industries and included drugstore chains, a super- market chain, pharmaceutical laboratories, airlines, a medical clinic, hotels, restaurant service companies, radio stations, sports teams, communications companies, construction firms, real estate firms, investment and financial companies, consulting companies, offshore firms, horse breeding farms and other agricultural businesses, mining operations, maritime agencies, and a department store." In the same year highly placed informants helped the Colombian authorities arrest six heads of the Cali Cartel although they carried on running the organisation from prison and by 2006 Drug Enforcement Administration ("DEA") and US Customs Agents were able to extradite the Rodriguez brothers.

Oficina de Envigado - Colombia

Largely seen as the inheritors of Pablo Escobar's drug trafficking empire, the Oficina de Envigado is now a collection of organisations that seeks alliances to operate. The Oficina de Envigado first arose as a faction of assassins established by Pablo Escobar in Envigado, a small municipality adjacent to Medellín, in the 1980s. Since then, the Oficina has evolved into a sizeable, drug running and extortion network operating from Medellín to the northern coast of Colombia and the Panamanian border area. It draws many of its leaders from former paramilitary blocs. It also controls some gambling and money laundering businesses and has ties to local police and other security officials. Much of the unrest in and around Medellín can be attributed to the Oficina.

The Oficina de Envigado's "Godfather" is Diego Fernando Murillo, alias 'Don Berna,' who after operating as a guerrilla fighter began working in the criminal underworld as an assassin ultimately controlled by Pablo Escobar. After Escobar's death, Murillo, took control over Medellín and established La Terraza, the Country's most feared hitman network. Murillo was arrested and imprisoned in 2005, when authorities connected him to the assassination of a local politician. Nonetheless, in prison Murillo found a safe haven where he could continue running his operations at a safe distance from his enemies, until he was extradited to the US in 2008, following which Oficina quickly splintered. One splinter group is the Paises, an armed wing of the Oficina.

North Coast Cartel - Colombia

The North Coast Cartel was based in the Colombian

city of Barranquilla by the Caribbean coast and was headed by Alberto Orlandez-Gamboa "Caracol" (the snail) considered as ruthless as Pablo Escobar.

The organisation transshipped significant amounts of cocaine to the US and Europe via the smuggling routes it controlled from Colombia's North Coast through the Caribbean. As head of the organisation, Gamboa depended on his close associates to conduct the organisation's operations and to insulate himself. As is typical with many Colombia-based organisations, Gamboa compartmentalised his business dealings. In addition, the success of Caracol's Barranquilla-based drug trafficking organisation was attributed, in part, to the respect the drug organisation received from other traffickers operating on Colombia's North Coast.

US DEA Intelligence indicated that traffickers paid taxes to Gamboa's organisation in order to be allowed to ship drugs out of the North Coast. His influence in this region was so strong that traffickers even asked him for permission before conducting assassinations. On June 6, In 1998, Caracol was arrested in Barranquilla on murder, kidnapping, and terrorism charges. He was extradited to the US in 2000, pleading guilty in 2003. With the capture of Gamboa the North Coast Cartel structure was dismantled by the Colombian National Police.

Norte del Valle Cartel - Colombia

The Norte del Valle Cartel, or North Valley Cartel, is a drug cartel which operates principally in the north of the Valle del Cauca Department of Colombia.

It rose to prominence during the second half of the 1990s, after the Cali Cartel and the Medellín Cartels fragmented, and was known as one of the most powerful organisations in the illegal drugs trade. The original leaders of the Norte del Valle cartel included Diego León Montoya Sánchez, Wilber Varela and Juan Carlos Ramírez Abadía, all of whom were killed by 2008. The Norte del Valle cartel is estimated to have exported more than 1.2 million pounds, or 500 metric tons, of cocaine worth in excess of US\$10bio from Colombia to Mexico and ultimately to the US for resale.

Indictments filed in the US charge the Norte del Valle cartel with using violence and brutality to further its goals, including the murder of rivals, individuals who failed to pay for cocaine, and associates who were believed to be working as informants. Leaders of the Norte del Valle cartel were further alleged to have bribed and corrupted Colombian law enforcement and Colombian legislators to, among other things, attempt to block the extradition of Colombian

narcotics traffickers to the US for further prosecution. According to the indictments filed in the US, members of the Norte del Valle cartel even conducted their own wiretaps in Colombia to intercept the communications of rival drug traffickers and Colombian and US law enforcement officials. The cartel is believed to have employed the services of the United Self-Defence Forces of Colombia (AUC) to protect the cartel's drug routes, its drug laboratories, and its members and associates.

Los Rastrojos - Colombia

Los Rastrojos first emerged in 2002 as the armed wing for one of the leaders of the Norte del Valle Cartel, is now involved in the Colombian armed conflict and is considered to be the largest supplier of drugs in Columbia although recent arrests and the emergence of rival factions are having a detrimental effect on their operation.

The Groups two main leaders, Javier Calle Serna, alias "Comba," and Diego Perez Henao, alias "Diego Rastrojo," were both captured in 2012. The loss of these bosses has left the group without a clear leadership, and other groups could take advantage to move into their territory. The group is primarily engaged in exporting cocaine to international markets, as well as extortion, gold mining and kidnapping at the local level. The Rastrojos move cocaine via go-fast boats and semi-submersibles from the Pacific side of their operations, and airplanes via the Venezuelan side. There is some evidence that these semi-submersibles may be being replaced by fully submersibles. In July 2010, authorities in Ecuador found a 33-meter submarine capable of moving at least 10 tons of cocaine. On the Venezuelan side, the airplanes appear to fly due north over Venezuelan territory, to avoid Colombian radar, until they are close to the Dominican Republic, then head due west until they reach Honduras or Guatemala where they land, offload and continue their journey north. They also use Venezuela as a bridge for cocaine moving towards Europe. They collaborate with a wide range of Mexican syndicates, including the most powerful the Sinaloa Cartel.

Los Rastrojos have more than 1,200 soldiers. Their strongholds are still in the area where they formed: Valle del Cauca and Cauca provinces along the Pacific coast.

For several years, the Rastrojos have had an agreement with the National Liberation Army (Ejercito de Liberacion Nacional - ELN) and with the Revolutionary Armed Forces of Colombia (Fuerzas Armadas Revolucionarias de Colombia - FARC) in certain other parts of the country. Both these alliances give the Rastrojos direct access to coca base -- the raw material

for cocaine -- at very cheap prices. Los Rastrojos' other main ally, Daniel Barrera Barrera, alias "El Loco," has struck similar agreements with the FARC in some areas.

Urabeños - Colombia

The Urabeños, also known as the Autodefensas Gaitanistas de Colombia, are currently one of the more ambitious and ruthless of Colombia's drug trafficking organisations. The Urabeños take their name from Urabá, a northwestern region near the Panamanian border highly prized by drug traffickers as it offers access to the Caribbean and Pacific coast, from the departments of Antioquia and Chocó. The Urabeños were founded by Daniel Rendón Herrera, better known as 'Don Mario,' an ex paramilitary in one of the many factions of the United Self-Defence Forces of Colombian (AUC). By avoiding infighting and paying their recruits well, the group has at times been able to steal territory from Los Rastrojos, their most hated rival. In 2009 a team of 200 police commandos captured Rendón on a farm in rural Urabá. Since Rendón's capture, the remnants of his organisation have fallen under control of the Usuga brothers, Juan de Dios and Dario Antonio, two former mid-ranking paramilitaries believed to have worked with Rendón since the 1990s. The two started out with an estimated 250 men following Rendón's arrest, and have since managed to grow exponentially.

In 2012, Juan de Dios was killed in a police raid on a ranch in Choco department. In a surprising display of strength, the Urabeños organised a series of coordinated strikes protesting his death in northern Antioquia, handing out fliers which referred to the group's former name, the Gaitanista Self-Defence Forces. The Urabeños also signalled their intention to respond aggressively to their leader's death when they publicly offered a US\$1,000 reward for each police officer killed in Antioquia, a public relations strategy best associated with kingpin Pablo Escobar.

Venezuela

Venezuela was one of three countries that emerged from the collapse of Gran Colombia in 1830 (the others being Ecuador and New Granada, which became Colombia). For most of the first half of the 20th century, Venezuela was ruled by military strongmen, who promoted the oil industry and allowed for some social reforms.

Whilst democratic governments have ruled Venezuela since 1959, it wasn't until Hugo Chavez was elected president from 1999 to 2013, that a new "21st Century Socialism," arose which purported to alleviate social ills while at the same time attacked the establishment

at home and western capitalism abroad in particular aggressively positioning Venezuela against the US and as a lightening rod for anti US sentiment in Latin America and beyond.

With the recent death of Chavez, it remains to be seen how this will affect the future of Venezuela albeit on the surface the regime has continued under successor Nicolas Maduro.

Current concerns include a weakening of democratic institutions, political polarization, a politicized military, rampant violent crime, over-dependence on the petroleum industry with its price fluctuations, and irresponsible mining operations that are endangering the rain forest and indigenous peoples.

Venezuela is a small-scale illicit producer of opium and coca for the processing of opiates and coca derivatives, however, large quantities of cocaine, heroin, and marijuana transit the country from Colombia bound for US and Europe. There is a significant narcotics-related money laundering operation in Venezuela, especially along the border with Colombia and on Margarita Island. Venezuela is also a source, transit, and destination country for men, women, and children subjected to sex trafficking and forced labour, with Venezuelan women and girls are trafficked within the country for sexual exploitation, lured from the nation's interior to urban and tourist areas; women from Colombia, Peru, Haiti, China, and South Africa are also reported to have been sexually exploited in Venezuela. Some Venezuelan women are transported to the Caribbean islands, particularly Aruba, Curacao, and Trinidad & Tobago, where they are subjected to forced prostitution; some Venezuelan children are forced to beg on the streets or work as domestic servants, while Ecuadorian children, who are often from indigenous communities, are subjected to forced labour.

Venezuela is subject to certain Sanctions and Embargoes. In 2008, US Office of Foreign Assets Control (OFAC) announced sanctions against 3 senior Venezuelan Military Commanders suspected by the USA as having contacts with the [FARC](#) exchanging arms for Drugs. The 3 Commanders are: Hugo Armando Carvajal Barrios, at the time the director of military intelligence; Henry de Jesus Rangel Silva, whom former President Chavez named general-in-chief and then defence minister in January 2012; Ramon Emilio Rodriguez Chacin, former Minister of Interior and Justice.

In September 2011, OFAC further sanctioned another four senior Venezuelan officials, following evidence retrieved from recovered FARC laptops acquired after a firefight in Colombia that suggested more involvement in arms for drugs. These are: Cliver Antonio Alcalá Cordon, later appointed as head of the army's Guiana Integral Strategic Defence Region (REDI Guayana); Congressman Freddy Alirio Bernal Rosales, a former Caracas mayor; Intelligence officer Ramon Isidro Madriz

Moreno; Amilcar Jesus Figueroa Salazar, a politician described as "a primary arms dealer for the [FARC](#), and ... a main conduit for FARC leaders based in Venezuela."³⁶ The most popular trafficking routes out of Venezuela are by air to the Dominican Republic and Honduras. Another route is to move the cocaine by land to Surinam, then by air or boat to West Africa and onwards to Europe. When moved by land, the cocaine is usually stored in local ranches and farms owned by civilian contacts. For more information on these and on the reasons these have been imposed see Part 1, Section 3, Sanctions & Embargoes above.

Cartel of the Suns - Venezuela

The term "Cartel of the Suns" (Cartel de los Soles) is used to describe groups inside Venezuela's military that traffic cocaine. The term "Cartel of the Sun" was reportedly first used in 1993 when two National Guard generals, were investigated for drug trafficking. As brigade commanders, each wore a single sun as insignia on their shoulders, giving rise to the name "Cartel of the Suns".

The elements of the military believed to be most deeply involved in Venezuela's drug trade are, unsurprisingly, concentrated along the western border with Colombia, especially the states of Apure, Zulia and Tachira. The power of these cells comes from their access to Venezuela's major airports, road checkpoints and ports, including Puerto Cabello in Carabobo state. These military organisations are thought to source some of their cocaine from Colombian guerrilla group the [FARC](#).

Walid Makled - Venezuela

It is suspected that the Cartel of the Suns also worked with civilian drug trafficker Walid Makled³⁷ in order to move their drug shipments out of Venezuela, before his arrest in Colombia in 2010. Walid was a member of one of Venezuela's most successful business families controlling supermarkets and appliance outlets to the ports and an airline. With many connections he would become for a time the most powerful civilian drug trafficker in Venezuela.

The beginning of Makled's decline came in 2008, with a political dispute with the Chavez camp. The political dispute is believed to have prompted the government's first serious effort to crack down on Makled's operations, trying to arrest him. Whilst he went into hiding he was found by Colombian forces and extradited back to Venezuela in 2010. After Walid's arrest, he went public with allegations about the Venezuelan establishment, stating, "All my business associates are generals." Since in custody he has chosen not to testify at his trial and is now silent.

The Bolivarian Liberation Forces (FBL) - Venezuela

The FBL are a guerrilla group based in western Venezuela, along the border with Colombia, that generally supported the government of former President Hugo Chavez, and has avoided confrontations with security

forces. The FBL first gained prominence in Venezuela in 1992, when it claimed responsibility for several attacks on public officials who were widely perceived as corrupt. According to the Venezuelan military, the FBL is led by an individual known as Jeronimo Paz, of whom little is known. The group is believed to have between 1,000 and 4,000 members, and is active mostly in the western border states of Apure, Tachira and Barinas although it also has a presence in the western states of Zulia, Merida, Portuguesa, Cojedes and Carabobo as well as in the capital city, Caracas. In Apure and Barinas, the FBL uses the densely forested San Camilo and Ticoporo nature reserves as its main hideouts.

The group funds itself mainly by kidnapping and extorting local landowners and businesses along the border with Colombia. In 2011, for instance, the FBL reportedly charged a group of oil workers in Apure a "protection fee" of 110,000 bolivars, or about US\$25,000.

Its financing activities have at times put the FBL in conflict with Colombia's [National Liberation Army \(ELN\)](#), which also operates on the border. It has had close relations with the larger [Revolutionary Armed Forces of Colombia \(FARC\)](#), which has provided the FBL with logistical support and training. The FBL does not currently pose anything like the same security threat in Venezuela as these Colombian rebel groups do in their country as it is largely pro-government.

Guyana/French Guyana & Suriname

The Guyana's were 5 colonies tied to major European powers, Spanish Guyana (now the Guayana Region in Venezuela), British Guyana (now Guyana), Dutch Guyana (now Suriname), French Guyana and Portuguese Guyana (now Amapá, a state in northern Brazil). French Guyana remains part of France whilst the two larger countries to the north and west, Guyana and Suriname, are independent.

Guyana, originally a Dutch colony in the 17th century, by 1815 Guyana had become a British possession. Guyana achieved independence from the UK in 1966, and since then it has been ruled mostly by socialist-oriented governments, with the current President Donald Ramotar Elected in 2011.

Guyana is a transshipment point for narcotics from South America - primarily Venezuela, to Europe and the US as well as being a producer of cannabis. Guyana is a source and destination country for men, women, and children subjected to sex trafficking and forced labour. Guyanese and foreign women and girls are forced into prostitution in Guyana and Guyanese children are

subjected to exploitative labour practices in the mining, agriculture, and forestry sectors as well as subjecting Indonesian workerfoot forced labour conditions on Guyanese-flagged fishing boats. Funds are increasingly laundered due to the drug trafficking and human smuggling.

Suriname was first explored by the Spaniards in the 16th century and then settled by the English in the mid-17th century, Suriname became a Dutch colony in 1667. Independence from the Netherlands was granted in 1975. Five years later the civilian government was replaced by a military regime that soon declared a socialist republic. A civilian administrations returned briefly in 1987, when international pressure finally forced a democratic election, but by 1990 the military overthrew the government and although a civilian coalition in today in power, it is a former military leader Desire Bouterse who has ruled since 2010.

Suriname is a source, destination, and transit country for women, men, and children who are subjected to sex trafficking and forced labour; women and girls from Suriname, Guyana, Brazil, and the Dominican Republic are subjected to sex trafficking in the country, sometimes around mining camps. Debt bondage and sex trafficking are reported to occur within the Chinese migrant community. Migrant workers in agriculture and on fishing boats and children working in informal urban sectors and gold mines are vulnerable to forced labour. As far as drugs are concerned, Suriname is an increasingly important transshipment point for South American drugs destined for Europe via the Netherlands and Brazil and a transshipment point for arms-for-drugs dealing.

First settled by the French in 1604, French Guyana is an overseas department and region of France. As an oversea region, it is officially inside the EU. French Guyana was the site of notorious penal settlements until 1951 which included the notorious Devil's Island. A large part of the department's economy derives from the presence of the Guyana Space Centre, established in 1964, French president Charles de Gaulle decided to construct a space-travel base to replace the Sahara base in Algeria and stimulate economic growth in French Guyana. It is now the European Space Agency's primary launch site near the equator.

French Guyana produces a small amount of marijuana grown for local consumption and is only considered a minor transshipment point to Europe.

Europe



Europe is the world's second-smallest continent by surface area, covering only about 2% of the Earth's surface and about 7% of its land area. Europe is the third-most populous continent after Asia and Africa, with a population of 733 million or about 11% of the world's population.

Europe, in particular Ancient Greece, is the birthplace of Western culture. In ancient Greek mythology, Europa was a Phoenician princess whom Zeus abducted after assuming the form of a dazzling white bull, taking her off to Crete. How it came to symbolise the geographic continent that it does today and has done since at least the 6th century BC is unclear. The term "Europe" then became used to designate not only a particular geography but a mechanism to distinguish the sphere of influence of the Western Church, as opposed to both the Eastern Orthodox churches and to the Islamic world. Europe is for our purposes divided into Eastern and Western Europe, with a focus on Russia and its close neighbours (for the "Stans" of Central Asia see Asia above) and the major core countries of the EU. Until the 20th century with significant immigration into Europe, the Europeans were mostly of white or pale skin and considered themselves Caucasians, after those that lived in the Caucasus of Southern Russia and North of Turkey. This because the term "Caucasian race," coined by the German philosopher Christoph Meiners in his *The Outline of History of Mankind* (1785), described those from the region as having the "whitest, most blooming and most delicate skin" and the concept of a Caucasian race linked to white skin was further developed by Johann Friedrich Blumenbach, a German professor of medicine. Basing his classification of the Caucasian race primarily on craniology, but also facial features, he defined five human races based on color, using popular racial terms of his day. He established caucasian as the "white race," as well as Mongoloid as the "yellow race," Malayan/"brown race," Ethiopian/"black race," American/"red race." Whilst there is no scholarly evidence of any such connection or race, many scientists maintained racial categorizations of color established by Meiners' and Blumenbach's works, well into the late 19th/20th centuries, increasingly used by Racists and in particular Nazi Germany as a justification for many of their abhorrent policies including the genocide of the Jews, world war and its aftermath.

Neo-Nazism - Europe and elsewhere

Neo-Nazism borrows elements from Nazi doctrine, including militant nationalism, racism, xenophobia, homophobia and anti-semitism. Holocaust denial is a

common feature, as is incorporation of Nazi symbols and admiration of Adolf Hitler. It is related to the white nationalist and white power skinhead movements in many countries. Neo-Nazi activity appears to be a global phenomenon, though many of the larger groups are European based. Some European and Latin American countries have laws prohibiting the expression of pro-Nazi, racist, anti-Semitic or anti-homosexual views. Many Nazi-related symbols are banned in European countries in an effort to curtail neo-Nazism. The main groups that espouse many or some of these neo-Nazi features include: the international network, Blood and Honour, including a splinter Belgium group called Blood, Soil, Honour and Loyalty; Combat 18 in the UK, Holland and elsewhere in Europe; the European Defence League (EDL) (being an offshoot of the English Defence League but since spawning Dutch Defence League, which is affiliated with the EFI, the European Freedom Initiative and the Norwegian Defence League as well as others. Of course in Norway the far right white supremacist Anders Behring Breivik killed 77 in the Oslo bombing/shooting massacre and was thought to be in favour of establishing the Norwegian Defence League. Elsewhere in Europe other far right groups include: the Bosnian Movement of National Pride; the Ustaše in Croatia; the MIÉP-Jobbik Third Way Alliance of Parties in Hungary; the Russian National Unity (RNE) and the Russian National Socialist Party; the Partei National Orientierter in Switzerland; the Nacionalni stroj (National Alignment) in Serbia; and the Swedish Resistance Movement. Whilst neo-Nazi organisations in France are outlawed, a significant number exist alongside far-right groups which include the Bloc identitaire, created by former members of the Unité Radicale group, close to National Bolshevism, Nouvelle Résistance (NR) and Troisième Voie (Third Way). Perhaps the most successful in political terms has been the Freedom Party of Austria (FPÖ), which won 33% of the vote in Carinthia and 22% in Vienna, also in 1994 in the Austrian election, the FPÖ won 22% of the vote. More recently the Greek far right political party Golden Dawn (Chrysi Ayi) is often labeled as neo-Nazi, although the group rejects this label. In the 2 elections in 2012, Golden Dawn received nearly 7% of the votes, entering the Greek parliament for the first time with around 20 representatives. Another Greek group which is considered as a neo-Nazi group is the Strasserite "Mavros Krinos" (Black Lily). Beyond Europe, the National Socialist Movement (NSM) is currently the largest neo-Nazi organisation in the US, which also is home to the Ku Klux Klan. The most significant attack carried out by a far right extremist is the Oklahoma bombing by Timothy McVeigh in 1995 killing 168. Elsewhere in North America, in Canada the Heritage Front and more recently the Nationalist Party of Canada are considered far right. In Asia, the National Socialist Japanese Workers Party and the Mongolian Tsagaan Khass are considered neo-Nazi groups as well. Even Israel has a far right movement called Patrol 36.

Eastern Europe



Whilst in modern times the political borders of Eastern Europe were largely defined and continue in popular perception by the Cold War, with the Iron Curtain separating the members of the Warsaw Pact from the European members of NATO and the polarization of Europe

as East-West. Famously, the iron curtain was popularized by Winston Churchill, who used it in his famous "Sinews of Peace" address in 1946 in Fulton, Missouri, who said, "From Stettin in the Baltic to Trieste in the Adriatic an iron curtain has descended across the Continent. Behind that line lie all the capitals of the ancient states of Central and Eastern Europe. Warsaw, Berlin, Prague, Vienna, Budapest, Belgrade, Bucharest and Sofia."

Beyond the Cold War divide, the distinction is sometimes illustrated by the fact that Eastern Europe is that part of Europe where the Cyrillic alphabet is used, for example: Cyprus, Serbia, Macedonia, Bulgaria, Ukraine, Belarus, and of course Russia and so the East-West differences predate the cold war, and originate in the history and the break up of the Roman Republic. As the power of Rome expanded, a cultural and linguistic division appeared between two halves of the Roman Empire, between the Western Roman Empire and the Eastern Roman Empire. Whilst the Western Roman Empire collapsed, being replaced by first the Frankish Empire under Charlemagne and then leading to the States of Western Europe, much of which we know today, by contrast the Eastern Roman Empire, mostly known as the Byzantine Empire, managed to survive and even to thrive for another 1,000 years, despite early conquest by the Mongols, but finally by the Muslim Ottoman Empire in the 15th century, which itself would be ruptured by the events of the First World War and the rise of the Soviet Union at the end of the Second World War.

The Iron Curtain that separated East and West was pulled apart in 1989, following the fall of the Berlin wall, as Eastern European countries which as so called satellite nations of Soviet Russia became independent. This was the final cataclysmic act for the Soviet Union which started in 1985 when Mikhail Gorbachev was elected general secretary of the Central Committee of the Communist Party and later President of the Soviet Union. His policy of Glasnost ("opening") and Perestroika ("change") would lead to the dissolution of the former Soviet Empire. Gorbachev's reforms accelerated and inevitably quickly resulted in the collapse of the supporting three pillars of the Soviet Empire, the

concentration of the constitutional powers with the Communist Party, Marxism-Leninism as the only permitted ideology and the centrally planned economy as the base of all economic activity. On 7 December 1991, in the forest of Belovezh in Belarus, the presidents of Russia, Ukraine and Belarus met. The meeting had not been prepared in advance, there was no agenda. Russian President Boris Yeltsin proposed to Stanislav Shushkevich, President of Belarus and President Leonid Kravchuk from the Ukraine to dissolve the Soviet Union. The three agreed and the Soviet Union was replaced by the Commonwealth of Independent States (CIS), a regional organisation composed of former Soviet Republics, but now importantly independent countries. Prior to this the Baltic States had declared their independence.

Baltic States

The three Baltic States; Latvia, Estonia and Lithuania; declared their independence in 1991 as the former Soviet Union crumbled, and for a time they prospered being nicknamed the "Baltic Tigers". Whist their economies have largely prospered, the financial crisis of 2008/2009 has taken its toll. They are also coming to terms with significant corruption, drug and organised crime problems. Estonia has one of the biggest drug problems in Europe. The moor landscape and vast forests host illegal drug laboratories which dedicate their activities over all to the production of synthetic drugs. Amphetamines and similar pills of doping effects are exported to much of Scandinavia. Experts estimate that 90% of the production of amphetamines goes through Finland to the rest of Northern Europe. From Russia Fentanyl is imported, a synthetic heroin. On the other hand the number of drug addicts in the country is high. According to the US State Dept Trafficking in Persons Report 2011; Estonia is also a 'source, transit, and destination country for women subjected to forced prostitution (in particular to Tallinn and the Northern European hemisphere), and for men and women subjected to conditions of forced labour' In Lithuania, corruption concerns are prevalent. According to the Heritage Foundation, over 50 government agencies are involved in the regulation of business and commerce, leading to businesses paying bribes to get permits and licences. In such an environment the black market is likely to also be a significant concern. According to the «Lithuanian Free Market Institute» 28 % of Lithuanian GDP came from the informal sector. Two fifths of the companies are involved in illegal activities, and or by not paying taxes. These tax related concerns are also mentioned by the US State Department Money Laundering Report 2012: "Most financial crimes, including VAT embezzlement, smuggling, illegal production and sale of alcohol, capital flight, and profit concealment, are tied to tax evasion by Lithuanians."

In Latvia surveys disclose that corruption is also an important concern for the citizens. A further area of concern relates to financial services in Latvia. Whilst the

US authorities had raised concern about Latvian Banks and their possible use by the [Russian Mafia](#) to transmit Russian funds via Latvia often through to Cyprus, the country had responded to tighten controls. Still during the so-called Euro crises and the collapse and part bail out of the Cypriot Banking sector, concerns have been raised once more, both in being a conduit in and out for Russian money, and operating a banking business model similar to that in Cyprus. The NGO Global Witness has criticized Latvia's KYC standards, claiming that they are not at a high enough standard, bearing the risk that the increased inflows into the banking system include funds from doubtful sources and reinforcing concern that the Russian mafia develops activities in the country. Latvia has four free trade zones.

Poland

Poland's history is one of conquest and counter conquest with the state of Poland establishing itself in the middle of the 10th century. By the mid-16th century, the Polish-Lithuanian Commonwealth ruled a vast tract of land in central and eastern Europe. During the 18th century, regional powers, Russia, Prussia and Austria partitioned Poland among themselves. Poland regained its independence in 1918 only to be overrun by Germany and the Soviet Union in World War II. It became a Soviet satellite state following the war, but its government was comparatively tolerant and progressive. Labour turmoil in 1980 led to the formation of the independent trade union "Solidarity" that over time became a political force with over ten million members. Free elections in 1989 and 1990 won Solidarity control of the parliament and the presidency, bringing the communist era to a close. Poland joined NATO in 1999 and the EU in 2004. With its transformation to a democratic, market-oriented country largely completed, Poland is an increasingly active member of Euro-Atlantic organisations. Whilst Poland is a minor transshipment point for Southwest Asian heroin and Latin American cocaine to Western Europe it is a major illicit producer of synthetic drugs for the international market.

Pruszkow Mafia - Poland

The Polish drugs trade is believed to be controlled by three main organised crime syndicates based in Gdansk and Warsaw. Most prominent amongst these three organisations is the Pruszkow Mafia, a group known to derive revenue from art and automobile theft, extortion, drug trafficking and prostitution. Human trafficking for the purposes of sexual exploitation, an industry flourishing in Poland, is another illegal activity in which the Pruszkow Mafia may be involved. Perhaps the most famous member of the Pruszkow Mafia is its former leader Andrzej Kolikowski, a figure who became in the 1990s Poland's most famous gangster. Kolikowski began his criminal career smuggling dollars, cars and other sought after goods from West Germany into communist Poland. Later, following the collapse of communist rule in Poland, Kolikowski formed a group of around

100 people to support his business operations. In 1992 this group amalgamated with the Pruszkow Mafia and Kolikowski became one of its leaders, investing in legal business avenues such as record labels, restaurants and nightclubs. Such legal commercial holdings were undoubtedly used to launder the proceeds of the group's criminal enterprise. In 2003 leaders of the Pruszkow Mafia were brought to trial in Warsaw. The prosecution succeeded only in securing relatively minor charges, ultimately failing in their endeavour to convict the group's leaders of murder, extortion, robbery and drug trafficking. During the trial connections emerged between the Pruszkow Mafia and politicians, such as Senator Aleksander Gawronik, dubbed the "treasurer of the Pruszkow".

Bulgaria

Bulgaria entered the EU on 1 January 2007 and soon after received lucrative EU subsidies. In July 2008 the surveillance report of the EU commission concluded that these subsidies are distributed by corrupt Bulgarian institutions which are riddled with members from organised crime. These criminal networks, were protected and connected inexorably with the political elite. In 2007 a parliamentary commission found that from the end of the communist period, whilst the rulers at the time had left office 139 former communist state intelligent agents were elected Members of Parliament, and that approximately 10% of the staff in public offices were connected to the former secret service with positions held in high positions of government and of State. It is no surprise that institutionalised corruption is a main issue of concern in Bulgaria.

The US State Department Money Laundering Report states in its 2012 edition that "corruption remains a serious problem and many still associate public tenders with kickbacks and money laundering. Financial crimes enforcement capacity is limited. The authorities opt for easy-to-prove, low-level corruption and related money laundering cases. As a result, progress on cases of high public interest, involving alleged siphoning of millions of taxpayer money, such as the public procurement of big energy infrastructure projects, have not generally been pursued. In 2011, casinos, night clubs, car dealerships and, to a lesser extent, wholesale traders, were the most common businesses associated with money laundering in Bulgaria. The tourism and gaming industries are considered important venues for money laundering activities among organised crime groups." According to the NGO Center for the Study of Democracy, alone the smuggling of cigarettes created an illicit income stream in excess of US\$400mio. in 2010-2011. In addition the US State Dept Narcotics Report 2012 observes that in Bulgaria as a transit country for heroin "Organised crime groups operating in Bulgaria have increased their influence and involvement in the international narcotics trade. These groups are sophisticated, well-financed, and entrenched within Bulgarian society. Bulgaria's Black

Sea ports continue to be exploited by drug traffickers to smuggle cocaine from South America to Europe and heroin from Turkey and Iran to Europe."

Balkans & Former Yugoslavia

The central Balkans, and what was the former Yugoslavia, were part of the Roman and Byzantine Empires before ethnic Serbs migrated to the territories of modern Serbia and Kosovo in the 7th century. During the medieval period, Kosovo became the center of a Serbian Empire and saw the construction of many important Serb religious sites, including many architecturally significant Serbian Orthodox monasteries. The defeat of Serbian forces at the Battle of Kosovo in 1389 led to five centuries of Ottoman rule during which large numbers of Turks and Albanians moved to Kosovo. By the end of the 19th century, Albanians replaced the Serbs as the dominant ethnic group in Kosovo. Serbia reacquired control over Kosovo from the Ottoman Empire during the First Balkan War of 1912. The Kingdom of Serbs, Croats, and Slovenes was formed in 1918; its name was changed to Yugoslavia in 1929. Various paramilitary bands resisted Nazi Germany's occupation and division of Yugoslavia from 1941 to 1945, but fought each other and ethnic opponents as much as the invaders. The military and political movement headed by Josip "TITO" Broz (Partisans) took full control of Yugoslavia when German and Croatian separatist forces were defeated in 1945. After World War II, Kosovo became an autonomous province of Serbia in the Socialist Federal Republic of Yugoslavia. Although communist, TITO's new government and his successors (he died in 1980) managed to steer their own path between the Warsaw Pact nations and the West for the next four and a half decades. In 1989, [Slobodan Milosevic](#) became President of the Republic of Serbia and his ultranationalist calls for Serbian domination led to the violent breakup of Yugoslavia along ethnic lines. In 1991, Croatia, Slovenia, and Macedonia declared independence, followed by Bosnia in 1992. See Bosnia below for more details. The remaining republics of Serbia and Montenegro declared a new Federal Republic of Yugoslavia in 1992 and under Milosevic's leadership, Serbia led various military campaigns to unite ethnic Serbs in neighboring republics into a "Greater Serbia." These actions were ultimately unsuccessful and led to the signing of the Dayton Peace Accords in 1995. In 1998, an ethnic Albanian insurgency in the formerly autonomous Serbian province of Kosovo provoked a Serbian counterinsurgency campaign that resulted in massacres and massive expulsions of ethnic Albanians living in Kosovo. The Milosevic government's rejection of a proposed international settlement led to NATO's bombing of Serbia in the spring of 1999, to the withdrawal of Serbian military and police forces from Kosovo in June 1999, and to the stationing of a NATO-led force in Kosovo to provide

a safe and secure environment for the region's ethnic communities. Elections in late 2000 led to the ouster of Milosevic and the installation of democratic government. In 2003, the FRY became Serbia and Montenegro, a loose federation of the two republics. See Kosovo below for more details.

Serbia

According to the US State Department Money Laundering Report for 2012 "corruption and organised crime continue to be significant problems in Serbia." The US State Dept Narcotics Report 2012 adds that "Serbia's Ministry of Interior believes Serbian organised crime groups primarily smuggle cocaine directly from South America to Western Europe. Serbia's predicament, can be traced to the dissolution of the former Yugoslavia, and its Countries leadership under [Slobodan Milosevic](#) and involvement in the Balkan wars that followed. Milosevic was accused by the International Criminal Tribunal for the former Yugoslavia in the Hague of committing crimes against humanity, but died in his cell before a verdict could be issued. During his time as President he fostered criminal networks to further Serbian expansionist aims in the region and the legacy of state sponsored criminality remains today. For more details see the case of [Slobodan Milosevic](#) in Part 2 Section 7 below.

Serbian Mafia - Serbia

The Serbian Mafia emerged under President [Slobodan Milosevic](#), who offered protection in return for political favours from members of the criminal underworld. The Serbian Mafia grew rapidly, generating large revenues from the smuggling of cigarettes, alcohol and oil in particular including sanctions busting. Despite the overthrow of Milosevic in 2000 and a period of bloody infighting between mafia bosses vying for power, the Serbian Mafia endured. According to the Serbian Interior Minister Mihajlovic in the early 2000s the Serbian Mafia was better armed and financed than both the Serbian Army and the Serbian Police. Connections between organised crime groups and the Serbian state also ran on into the early years of the 21st century, with Prime Minister Zoran Dindic assassinated by the Serbian Mafia in response. The government launched Operation Sabre in an attempt to purge criminal influence from state machinery; it led to more than 10,000 arrests, testifying to the size of the Serbian Mafia. Amongst the high profile figures arrested was Milan Sarajlic, Serbia's Deputy State Prosecutor, who confessed to being paid by the Zemun clan (a Belgrade sect within the Serbian Mafia). Today, five major clans are today thought to dominate the Serbian Mafia. Main Paramilitary Serbian Groups. Involved in the War

in Bosnia and in Kosovo and accused of ethnic cleansing include the Serbian Guard; the White Eagles; the Serb Volunteer Guard, also known as Arkan's Tigers; the Scorpions; the Yellow Wasps and the Wolves of Vučjak.

Bosnia & Herzegovina

Bosnia and Herzegovina declared independence from the former Yugoslavia in 1992, though ethnic Bosnian Serbs, responded, and supported by neighboring Serbia and Montenegro, with armed resistance aimed at partitioning the republic along ethnic lines and joining Serb-held areas to form a "Greater Serbia." In 1995 after (insert Sarajevo and Islam connections), the warring parties agreed a peace deal which retained Bosnia and Herzegovina's international boundaries and created a multi-ethnic and democratic government charged with conducting foreign, diplomatic, and fiscal policy.

In March 2002, Bosnian authorities raided the offices of Benevolence International Foundation (BIF) due to suspected funding of Al-Qaeda in Sarajevo, and they uncovered a handwritten list containing the name of twenty wealthy donors sympathetic to Al-Qaeda. The list, referred to as "The Golden Chain," contained both the names of the donors including many wealthy Saudi businessmen and the names of the recipients (but does not mention amounts given). It is thought the letter was written in 1988 or 1989. Seven of the payments are made to bin Laden. Al-Qaeda was formed in late-1988. The Wall Street Journal later commented that, "The list doesn't show any continuing support for Al-Qaeda after the organisation began targeting Americans, but a number of the Saudis on it have been under scrutiny by US officials as to whether they have supported terrorism in recent years."

Bosnia is considered a transit point for heroin being trafficked to Western Europe and a minor transit point for marijuana. Bosnia remains highly vulnerable to money laundering activity given a primarily cash-based and unregulated economy, weak law enforcement, and instances of corruption.

Bosnian Mujahideen - Bosnia

Bosnian Mujahideen were foreign Muslim volunteers who fought in Bosnia with the aim of fighting for Islam and on behalf of Muslims under attack from Serbs during the 1992–95 Bosnian War. The number of volunteers throughout the war is still disputed, from around 300 to 6,000. These foreign Muslim Jihad or "Islamic holy warriors" were assembled in a special Bosnian Army unit called the "El Mujahed unit". This unit committed some of the worst war crimes and crimes against humanity against Bosnian Serb and Bosnian Croat civilians and POWs. According to the US 9/11 Commission Report, the commander of the Bosnian Muslim unit "El Mujahed" was Abu Abdel Aziz "Barbaros", described as a "senior Al-Qaeda recruiter" was born in Saudi Arabia in 1942. He was a veteran of the Mujahideen in Afghani-

stan. He was an early member of the Al-Qaeda movement established by bin Laden and Abdullah Azzam. He was made the amir, or military commander of the Saudi Arabian and Afghani Mujahideen in Bosnia. The foreign Mujahideen arrived in central Bosnia in the second half of 1992 mostly coming from North Africa, the Near East and the Middle East.

Former US Balkans peace negotiator Richard Holbrooke said in an interview that he thought "the Muslims wouldn't have survived without this" help, as at the time a U.N. arms embargo diminished the Bosnian government's fighting capabilities. In 2001, Holbrooke called the arrival of the Mujahideen "a pact with the devil" from which Bosnia still is recovering.

Kosovo

Albanian nationalism within Kosovo as part of the former Yugoslavia increased in the 1980s, which led to riots and calls for Kosovo's independence. At the same time, Serb nationalist leaders, such as Slobodan Milošević, exploited Kosovo Serb claims of maltreatment to secure votes from supporters, many of whom viewed Kosovo as their cultural heartland. Under Milošević's leadership, Serbia revoked Kosovo's status as an autonomous province of Serbia and carried out repressive measures against the Kosovar Albanians. Albanians created the Kosovo Liberation Army and launched an insurgency and paramilitary forces under Milošević conducted a brutal counterinsurgency.

The Milošević government's rejection of a proposed international settlement led to NATO's bombing of Serbia in the spring of 1999, to the withdrawal of Serbian military and police forces from Kosovo in June 1999, and to the stationing of a NATO-led force in Kosovo to provide a safe and secure environment for the region's ethnic communities. In 2004 the international community opened negotiations on the future status of Kosovo and in 2008, after years of inconclusive negotiations, the UN-administered province of Kosovo declared itself independent of Serbia.

Kosovo has porous borders which facilitate an active black market for smuggled consumer goods, especially fuels, cigarettes and pirated products, largely along the Kosovo-Serbian border. Kosovo is a largely a transit point for illicit drugs and not a destination point. Illegal proceeds from domestic and foreign criminal activity are generated from official corruption, tax evasion, customs fraud, organised crime, contraband, and other types of financial crimes. Corruption is a significant problem. Most of the proceeds from smuggling activity are believed to be laundered directly into the economy in areas such as construction and real estate, retail and commercial stores, banks, financial services, casinos and trading companies, with smaller amounts laundered through the financial system.

Kosovo Liberation Army - Kosovo

The Kosovo Liberation Army (KLA) formed in Macedonia in 1992 with the goal of uniting the ethnic Albanian populations of Albania, Kosovo and Macedonia into a "Greater Albania." Their name recognised that the province of Kosovo, officially part of the new nation of Serbia, was their most important and difficult target. The KLA remained basically unknown until 1995, when it began carrying out small arms and sabotage attacks against Serbian Police outposts in Kosovo. The KLA also conducted vicious reprisal attacks against Kosovars accused of co-operating with the Serbians. The escalating violence forced the Serbian government to respond, but their response was, by almost any standard, far too aggressive; many innocent men, women and children died as a result.

As the Serbian crackdown against the KLA grew increasingly brutal, the group's ranks swelled. An organisation that began in 1998 with no more than 500 members was estimated to be 12,000 to 20,000 strong by the beginning of 1999. Funding came from Kosovar Albanians in Kosovo and Albanians abroad as well as from the proceeds from Some drug-trafficking and organised crime. When the US-led coalition attacked Serbia in defense of the Kosovars in January 1999, the appearance of imminent victory drew even more ethnic Albanians to the KLA flag. The KLA militias played a critical role in the coalition victory, forcing Serbian forces out into the open where American and allied airpower could punish them. Since the end of the war in Kosovo, the KLA has become largely inactive though there remains a small core of hard liners still dreaming of a greater Albania.

Albania

Albania declared its independence from the Ottoman Empire in 1912, but was conquered by Italy in 1939 and by Communists in 1944. Albania allied itself first with the USSR (until 1960), and then with China (to 1978). In the early 1990s, Albania ended 46 years of communist rule and established a multiparty democracy. The transition has proven challenging due to widespread corruption and powerful organised crime networks. Slow progress is being made with elections resulted in a coalition government in 2009, the first such in the country's history. Albania joined NATO the same year and is a potential candidate for EU accession. Although Albania's economy continues to grow, the country is still one of the poorest in Europe, hampered by a large informal economy. Albania also has a large cash economy and significant money flows from abroad in the form of remittances. Albania has a significant black market for certain smuggled goods, mainly tobacco, jewelry, stolen cars, and mobile phones, due to its high level of consumer imports and weak customs controls. Albania is a transit country for Afghan heroin smuggled to Western Europe and serves as a key gateway for heroin distribution throughout Europe. Local

production of marijuana is also on the rise for domestic and European use. Albania serves as a base of operations for regional organised crime organisations as illicit proceeds are easily laundered, with real estate and business development projects being the most popular methods. Terrorist financing also remains a threat in Albania.

Albanian Mafia - Albania

In Albania there are over 15 mafia clans that control organised crime. The Albanian Mafia have constructed an enormous crime syndicate that is primarily based around drugs and arms trafficking. However, the syndicate participates in a diverse range of criminal enterprises, including car theft. Similar to other organised crime groups, the typical structure of the Albanian Mafia is hierarchical. They hold a deep reliance on loyalty, honor, and blood relationships. Albanian Mafia clans are usually made up of groups of fewer than 500 members. They are secretive and little information is known about the current Albanian Mafia bosses, though it is believed that Daut Kadriovski is one of the leaders. He is the reputed boss (godfather) of one of the 15 Mafia clans and whilst he remains at large he is wanted by the authorities in many Countries.

In the 1980s, the Albanian Mafia moved into New York and began to fight with the Italians. Today, the Albanian presence is highly evident and the organisation has come to an agreement with other criminal syndicates, who have agreed to stay out of their way. In Italy, Albanian organised crime gangs appear to control the car theft and trafficking market. Albanian gangs are believed to be largely responsible for sex trafficking, immigrants smuggling, and the heroin trade in the UK. They hold a heavy presence in France, Switzerland, Canada, Belgium, Germany, Australia, and Honduras. Whilst Albanian criminal gangs had long existed they were a scattered and disorganised band of gangs, largely working for others. This changed though through a number of important developments which transformed them from local criminal gangs into international major operators to rival those in Russia, Italy and elsewhere. Firstly the campaign against the Italian Mafia by for example US Law Enforcement provided an opportunity for others, including the Albanians to take up part of the drug trade previously controlled by the Italians. Secondly, the civil war in Yugoslavia and in particular the fight for Kosovo with its large ethnic Albanian population provided a unique opportunity to profit from the chaos and engage in illegal activities, including, large scale arms trading, goods and refugee smuggling and fund raising through increased and or diverted drug trafficking. Approximately 60% of Western Europe's heroin trade was disrupted as a result.

A great source of recruitment and local knowledge and support comes from the émigré communities located throughout Western Europe. Whether in Italy, Austria, Germany, or Switzerland, ethnics from Kosovo, Macedonia, and Albania, have been sought out by organised crime groups for criminal activity. Those from

the former Yugoslavia, especially, having fled during the outbreak of civil war, were taken into the capitals of Western Europe as political refugees. As their numbers swelled, these unemployed refugees, unable to obtain government assistance, found that there was money to be made in organised crime. Many were taken on as cheap labour in restaurants, cafes, and the like. Once there, they were given places to stay, false papers, and paid in cash. Beholden to the Albanian Mafia already many were recruited for organised crime groups operating in the region. Their familiarity with Kosovo, Macedonia, and Albania made them naturals for ferrying contraband back and forth.

Nano Aldo Bare - Albania

The Nano Aldo Bare are Albania's most notorious crime gang led by Alfred Shkurti with main operations in Albania, Turkey, Bulgaria, Macedonia and Romania, trafficking drugs into Western Europe. The gang is reputed to be extremely dangerous and violent and have close connections with the Turkish Mafia, particularly, the Ulkuculer.

Belarus

Once part of the early Russian empire, known as the Kyivan Rus, Belarus was gradually taken over by Lithuania in the 14th century and became part of the Polish-Lithuanian Grand Duchy. Belarus means white Russians. The Scandinavians who moved in the east were called Rus and from them came the word Russia, see Russia below. During the Mongol era, the Russians were classified into three different groups: Belarusians (white Russians), little Russians, and great Russians. The name Belarus and the country evolved from Belarusians. It was to be 400 years before Belarus came under Russian control again but notwithstanding Belarus formal independence from the USSR in 1991 it has retained closer political and economic ties to Russia than any of the other former Soviet republics, though recently these ties have become strained as once cheap Russian gas prices have given way to market pricing, and Belarus under the autocratic and authoritarian President Alexander Lukashenko, in power since 2004, a former collective-farm director, unable to pay, with an unreformed economy and a political system stuck in Soviet thinking. Belarus is home to nearly 10 million people, with the largest city Minsk also its capital. The country was proclaimed as an 'outpost of tyranny' by former US Secretary of State Condoleezza Rice and since then sanctions have been imposed on the President and those to him by both the US and the EU for political corruption, restrictions on freedoms and human rights abuses. For more details on Sanctions and Embargoes see Part 1, Section 3 above.

Belarus is considered as one of the most corrupt countries in the world by Transparency International being rated 123 out of 175. Belarus is both a source and a transit country for trafficked persons, primarily women. Information from the Netherlands, Lithuania,

and Bosnia, refer to Belarus as a country of origin for women being trafficked to or through their countries. Women from Russia, Ukraine and Lithuania are trafficked through Belarus to countries in Europe, primarily Germany and Poland. Other anecdotal evidence suggests that the Russian Mafia is active in trafficking young women to Cyprus, Greece, Israel, and Western Europe. The Ministry of Internal Affairs acknowledges that Russian criminal organisations actively may try to recruit and lure women into serving as prostitutes in Western Europe and the Middle East. Traffickers, who are associated with organised crime and drug trafficking, entice their victims through advertisements for lucrative jobs in newspapers and on the Internet. Belarus' location between Russia and the West combined with its good rail and road transportation systems and a customs union with Russia that eliminates internal borders between the two countries adds to Belarus' attractiveness as a drug transit corridor, into or via Russia, and to the Baltics and Western Europe. Belarus also faces many organised crime problems that plague other countries of the former Soviet Union.

Ukraine

Ukraine, a country of almost 48 million people, was the centre of the first eastern Slavic state, Kyivan Rus, which during the 10th and 11th centuries was the largest and most powerful state in Europe. After being incorporated into the Grand Duchy of Lithuania and eventually into the Polish-Lithuanian Commonwealth, Ukraine would come under the Protectorate of Russian rule, in 1654, where the then Cossack Hetmanate was established. This would last through tsarist Russian rule and throughout the time of the Soviet Union until Ukraine truly gained its independence in 1991. Still from independence until today, Ukraine remains split in its loyalties, with the Russian speaking industrial east remaining largely loyal to Kremlin backed political candidates, and the more Ukrainian speaking west supporting independent candidates looking more towards the EU and the US for its future. As a consequence Ukrainian politics has swung between the two which, together with the prevalence of organised crime, has led to a deterioration in the reputation of the Ukraine.

In the Presidential campaign of 2004, the eventual winner, Viktor Yushchenko, was poisoned with dioxin, leaving him disfigured. Subsequent internal squabbles in the Yushchenko camp allowed his rival Viktor Yanukovych to stage a comeback in parliamentary elections and become prime minister in 2006. An early legislative election, brought on by a political crisis in the spring of 2007, saw Yuliya Tymoshenko, as head of an "Orange" coalition, installed as a new prime minister

in 2007. Viktor Yanukovych was elected President in a February 2010 run-off election that observers assessed as meeting most international standards. The following month, Ukraine's parliament, the Rada, approved a vote of no-confidence prompting Yuliya Tymoshenko to resign, from her post as prime minister and thereafter she would be imprisoned on abuse of office charges in connection with gas contracts, widely considered trumped up by many commentators, particularly in the EU and the US. There had been running a serious dispute between Russia and Ukraine on the supply and distribution of gas, with Yulia Tymoshenko openly accusing the two States' joint venture, RosUkrEnergo, of being partly owned by Semyon Mogilevich; with the inference being that the former President Leonid Kuchma, a political supporter of Viktor Yanukovych allegedly therefore complicit in providing the Ukrainian holding to the Russian mafia leader.

As similar to the development of the Russian economy after the collapse of the USSR in 1991, much of the Ukrainian extractive industries, now concentrated on Ukrainian business leaders and so called Ukrainian oligarchs have been afflicted by varying levels of corruption and involvement by organised crime throughout the 1990s. As a result of its geographic position, the Ukraine is used as a transshipment point for opiates and other illicit drugs from Africa, Latin America, and Turkey to Europe, Russia and other parts of the former USSR. Ukraine is a source, transit and increasingly, destination country for men, women, and children subjected to forced labour and sex trafficking. Ukrainian victims are sex trafficked within Ukraine as well as in Russia, Europe and the Middle East. An Internal Organisation for Migration survey released in 2006 concluded that since 1991, approximately 117,000 Ukrainians had been forced into exploitative situations in Europe, the Middle East, and Russia.

Moldova

One of the poorest nations in Europe, Moldova was incorporated into Romania during the interwar period, and then incorporated into the Soviet Union at the close of World War II. Whilst gaining independence in 1991, Moldova remained heavily influenced by Russia, even electing a communist, Vladimir Voronin, as its president in 2001, who served until 2009, being replaced by four Moldovan opposition parties, namely the Alliance for European Integration (AEI). Moldova is a transshipment point for illicit drugs from Southwest Asia via Central Asia to Russia, Western Europe, and possibly the US. In Moldova crime is widespread and their is a large underground economy.

Hungary

Hungary became a Christian kingdom in A.D. 1000 and for many centuries served as a bulwark against Ottoman Turkish expansion in Europe and formed part of the Austro-Hungarian Empire, which collapsed during World War I. The country fell under communist rule following World War II. In 1956, a revolt and an announced withdrawal from the Warsaw Pact were met with a massive military intervention by Moscow. Hungary achieved its independence with the demise of the Soviet Union holding multiparty elections in 1990, joining NATO in 1999 and the EU five years later in 2006. Hungary is a transhipment point for Southwest Asian heroin and cannabis and for South American cocaine destined for Western Europe. Hungary is a limited producer of precursor chemicals, particularly for amphetamine and methamphetamine and a significant consumer of ecstasy. Hungary remains vulnerable to money laundering, related to organised crime and drug trafficking.

Romania

Romania as a State was formed and gained recognition after uniting a number of principalities in 1878 securing autonomy outside the Ottoman empire. It was on the winning side in World War I and gained territory, most notably Transylvania and the losing side in World War 2 being overrun by the Soviets. The post-war Soviet Republic would be ruled by long term dictator Nicolae Ceausescu who took power in 1965 and ruled through oppressive and draconian measures until he was overthrown and executed in late 1989. Former communists dominated the government until 1996 when they were swept from power. Romania joined NATO in 2004 and the EU in 2007. Romania is a major transshipment point for Southwest Asian heroin transiting the Balkan route and small amounts of Latin American cocaine bound for Western Europe.

Transcaucasus Region

The Transcaucasus is bordered on the north by Russia, on the west by the Black Sea and Turkey, on the east by the Caspian Sea, and on the south by Iran. It includes part of the Caucasus Mountain, Armenia, Azerbaijan and Georgia, and borders the northern portion of the Caucasus which is known as the Ciscaucasus and is part of Southwestern Russian. The Ciscaucasus includes the autonomous republics of Adygea, Karachay-Cherkessia, Kabardino-

Balkaria, North Ossetia, Ingushetia, Chechnya, and Dagestan. Three territories in the region claim independence but are recognised as such by only a handful or by no independent states, namely; Abkhazia, Nagorno-Karabakh and South Ossetia. Together the Transcaucasus and the Ciscaucasus make up the region known as the Caucasus. In Greek mythology the Caucasus, was one of the pillars supporting the world. After presenting man with the gift of fire, Prometheus was chained there by Zeus, to have his liver eaten daily by an eagle as punishment for defying Zeus' wish of not giving the "secret of fire" to humans. Located on the peripheries of Turkey, Iran, and Russia, the region has been an arena for political, military, religious, and cultural rivalries and expansionism for centuries. Throughout its history, the Caucasus was usually incorporated into the Persian world. The region would though be conquered by the Ottomans, the Mongols, local kingdoms and khanates, as well as, once again, Persia, until its subsequent conquest by Russia.

Armenia

Armenia prides itself on being the first nation to formally adopt Christianity (early 4th century). Due to its location it has enjoyed periods of autonomy and endured rule by powerful neighboring empires. As part of the Ottoman empire, the Armenians were provided with a large degree of autonomy and relative religious freedom. During World War I with Ottoman Turk rule unravelling, Greece, Bulgaria and Serbia left the empire and with the Armenians assisting opposing Allied Russian forces, the Ottoman Turks reacted with brutal force that resulted in 1.5 million Armenian deaths from a total of 2.5 million. The actions by the Ottoman Turks predate the genocide committed against the Jews by Nazi German decades later. Whilst most of the world have acknowledged these acts as genocide, a few still do not, including most importantly Turkey. Armenia was conquered soon after by the Soviet Red Army and remained part of the Soviet Union until its break up, achieving independence in 1991. The major issue in the region is the dispute with Azerbaijan over the disputed region Nagorno-Karabakh, a primarily Armenian-populated region, within Azerbaijan, where a short war was fought between the two in 1988. By 1994, when a cease-fire took hold, ethnic Armenian forces held not only Nagorno-Karabakh but also a significant portion of Azerbaijan proper. Armenia grows a small amount of cannabis for domestic consumption, is a minor transit point for illicit drugs, mostly opium and hashish moving from Southwest Asia to Russia and to a lesser extent the rest of Europe.

Azerbaijan

Azerbaijan is a nation with a majority-Turkic and majority-Shia Muslim population with a similar history to that of Armenia and the wider region, joining the Soviet Union after World War I and achieving independence after the fall of the Soviet Union in 1991. Its conflict with Armenia (see above) is not fully resolved. Corruption in the country is widespread, and the government, which eliminated presidential term limits in a 2009 referendum, has been accused of authoritarianism. Azerbaijan grows cannabis and opium poppy, mostly for CIS consumption and is a transit point for Southwest Asian opiates bound for Russia and to a lesser extent the rest of Europe.

Georgia

Like Armenia and Azerbaijan, Georgia has a similar history and joined the Soviet Union after World War I, achieving independence after the fall of the Soviet Union in 1991. Mounting public discontent over rampant corruption and ineffective government services, followed by an attempt by the incumbent Georgian Government to manipulate national legislative elections in November 2003 led to widespread protests that led to the resignation of Eduard Shevardnadze, President since 1995 and former Foreign Secretary of the Soviet Union.

In the aftermath of that popular movement, which became known as the "Rose Revolution," new elections in early 2004 swept reformist Mikheil Saakashvili into power. With tensions strained with Russia and with Russian assistance and support to the separatist regions of Abkhazia and South Ossetia, periodic flare-ups in tension and violence culminated in a five-day conflict in August 2008 between Russia and Georgia, including the invasion of large portions of undisputed Georgian territory. Russian troops pledged to pull back from most occupied Georgian territory, but in late August 2008 Russia unilaterally recognised the independence of Abkhazia and South Ossetia, and Russian military forces remain in those regions. Today a political fight between billionaire philanthropist Bidzina Ivanishvili and the President continues with each vying for overall control. Georgia grows cannabis and opium poppy, mostly for CIS consumption and is a transit point for Southwest Asian opiates bound for Russia and to a lesser extent the rest of Europe.

Russia



Russia is the largest country in the world, covering more than one-eighth of the Earth's inhabited land area. Russia is also the world's most populous nation with 143 million people as of 2012. Extending across the entirety of northern Asia and much

of Eastern Europe, Russia spans nine time zones and incorporates a wide range of environments and landforms. The nation's history began with four tribes, the Chuds, Slavs, Merians and Krivichs who lived in the region emerging as recognisable group's in Europe between the 3rd and 8th centuries AD but who were first conquered by a Finnic warrior elite tribe called the Varangians or the Rus, derived from an old Norse term for "the men who row" as rowing was the main method of navigating the rivers of Eastern Europe. The tribes freed themselves by working together but then fought amongst themselves. The result allowed the Varangians, or the Rus, to return, largely welcomed by the tribes to bring peace and stability to the region. As a result the medieval state of Rus arose in the 9th century. In 988 the Rus adopted Orthodox Christianity from the Byzantine Empire, beginning the synthesis of Byzantine and Slavic cultures that defined Russian culture for the next millennium. Rus' ultimately disintegrated into a number of smaller states and became easy prey for the Mongols. One of the leading successor Rus' states, known as the Grand Duchy of Moscow emerged in the 12th Century and gradually reunified the surrounding Rus principalities, achieving independence from the Mongols after 200 years of Mongol domination (13th-15th centuries), gradually conquering and absorbing surrounding principalities. By the 15th century, the ruler of the Grand Duchy of Moscow, Ivan III of Moscow was the first local ruler to become universally recognised under the title Grand Duke of all Rus'. In the early 17th century, a new Romanov Dynasty continued to expand across Siberia to the Pacific. Under Peter I (1682-1725), further lands were conquered extending to the Baltic Sea and the country was renamed the Russian Empire, which was the third largest empire in history, stretching from Poland in Europe to Alaska in North America.

During the 19th century, more territorial acquisitions were made in Europe and Asia. Defeat first in the Russo-Japanese War of 1904-05 followed by repeated

devastating defeats of the Russian army in World War I led to widespread rioting in the major cities of the Russian Empire and to the overthrow in 1917 of the imperial household. The communists under Vladimir Lenin seized power soon after and formed the USSR. Lenin was succeeded by Josef Stalin (1928-53) who strengthened communist rule, helped defeat Nazi Germany and consolidated Russian authority and dominance within the Soviet Union at a cost of tens of millions of lives.

The Soviet economy and society stagnated in the following decades until leader Mikhail Gorbachev (1985-91) introduced glasnost (openness) and perestroika (restructuring) in an attempt to modernize communism, but his initiatives inadvertently released forces that by December 1991 splintered the USSR into Russia and 14 other independent republics. Since then, Russia has attempted to modernize, experiencing democratic reforms under President Yeltsin but under his successor President Putin, Russia is considered by many very much a centralized semi-authoritarian state, albeit one which has achieved significant economic growth and severely disabled a Chechen rebel movement, although violence still occurs throughout the North Caucasus and Chechnya. The radical transformation to a post Soviet existence saw the rise of the Russian Oligarchs;³⁸ as well as the rise of organised crime and corruption much of which continues to this day and remains a significant threat to the proper functioning of the Russian State. The Russian Mafia, particularly the Solntsevskaya Bratva and Tambov Syndicate and thousands more smaller outfits are prevalent and engage in a broad range of illegal activities, particularly extortion, drug trafficking, oil and gas smuggling and human trafficking, political corruption and the smuggling of weapons and even nuclear material. Particularly successful is the Chechen Mafia.

Russia remains concerned about the smuggling of poppy derivatives from Afghanistan through Central Asian countries with Russia used as a trans-shipment and destination point for Asian opiates, cannabis, and Latin American cocaine bound for growing domestic markets, and to a lesser extent Western and Central Europe, and occasionally to the US; Russia is also a major source of heroin precursor chemicals corruption and organised crime are key concerns. There is also a limited cultivation of illicit cannabis and opium poppy within Russia itself as well as production of methamphetamine, mostly for domestic consumption. Russia is a source, transit, and destination country for men, women, and children who are subjected to forced labour and sex trafficking.

There has been a sustained series of terrorist attacks with a considerable number of casualties since the outbreak of the First Chechen war which include: [1973 - Aeroflot Tu-104 \(100\)](#), [1996 - hostage taking in Budennovsk, Russia, by Chechen Rebels \(143\)](#) [1999 - apartment bombings in Moscow Russia \(301\)](#) [2002 - Theater Hostage Crisis, Moscow, Russia by Chechen Rebels \(168\)](#) [2003 - Red Square bombing in Moscow \(6\)](#) [2004 - School Hostage Crisis, Beslan Russia by Chechen Rebels \(366\)](#) [2004 - Akhmad Kadyrov \(President of Chechnya\) assassinated](#) [2004 - Volga-Avia Express Flight 1303 \(89\)](#) [2010 - Metro bombings in Moscow Russia by Islamist Chechen terrorists \(40\)](#).

Russian Designated Terrorist Organisations

Russia have designated a number of organisations as terrorist organisations, focussing on those that pose a threat in some way to the Russian State with a real focus on Chechnya and the North Caucasus, in particular the umbrella group called the [Caucuses Emirate](#). For more details of terrorist groups operating in or from this area see North Caucasus/Ciscaucasus below. Russia has also designated organisations involved in either financing or advocating the insurgency in the North Caucasus. These groups include [Jamaat-e-Islami](#), [Hizb-ut-Tahrir](#), the [Muslim Brotherhood](#) and Islamic charities such as [Jamiat al-Islah al-Ijtimal \(the Society of Social Reforms\)](#), [Jamiat Ihya al-Turaz al-Islami \(the Society for the Revival of the Islamic Heritage\)](#), both based in Kuwait and [Al-Haramain Islamic Foundation](#). Beyond, but still linked to, the North Caucasus, external Islamic groups have been designated including the [Islamic Party of Turkestan](#), formerly known as the [Islamic Movement of Uzbekistan \(IMU\)](#) and its breakaway faction the [Islamic Jihad Group \(IJG\)](#). These groups are reportedly seeking to establish an Islamic caliphate in Central Asia. They are also alleged to have insurgent ties in Chechnya and the other parts of the North Caucasus.

[Al-Qaeda](#) and the [Taliban](#) also appear on the Russian list, both said to have trained fighters for Chechnya as well as the [Egyptian Islamic Jihad](#) and [al-Gama'a al Islamiyya](#). The Egyptian groups are featured on the list, because they formed the core of recruits of the original Al-Qaeda in the 1990s. Also included are [Asbar al-Ansar](#) and [Jund Ash Sham](#), [AQ](#) affiliates operating in Lebanon and Syria. The Pakistani-based [Laskhar-e-Toiba](#) is also on the list. The group has been fighting for Kashmiri independence from India or a merger with Pakistan in a long and bloody conflict. Its propaganda material includes one pamphlet entitled "Why are we waging Jihad," which identifies Chechnya as a key area of international interest. The group has maintained active collaboration with fighters in Chechnya.

Special Focus 18 Russian Mafia - Russia



The Russian Mafia engages in a broad range of illegal activities, particularly extortion but also drug trafficking, oil and gas smuggling and human trafficking, political corruption and smuggling of weapons and nuclear material.

The Russian Mafia has its origins in the vory-v-zakone (thieves with a code of honor), a society of thieves that evolved during the era of Imperial Russia. This society was fully formed by the time of Stalin's era at the gulags where the criminals were sent as a punishment. The criminal groups operated a black economy during the 1970s avoiding and bypassing the Communist State. Whilst the criminal groups had refused to cooperate with the state, this began to change as the new criminal class teamed up with corrupt officials, army officers and politicians to steal State assets, particularly after 1991 and the collapse of the Soviet Union.

As the Soviet Union collapsed, so too did the economy, directly affecting most of the government workers. Desperate for money, many former government workers turned to crime, others joined the former Soviet citizens who moved overseas, and the Russian Mafia became a natural extension of this trend. Former KGB agents, military men and veterans of the Afghan and First and Second Chechen Wars, now finding themselves out-of-work but with experience in areas which could prove useful in crime, joined the increasing crime wave. Widespread corruption, poverty and distrust of authorities only contributed to the rise of organised crime. Contract killings, bombings and kidnappings reached an all-time high with many gangland murders taking place, a substantial number remaining unsolved.

By 1993 many banks in Russia were owned by the mafia, and most businesses were paying protection money. In that year, 1400 people were murdered in Moscow, crime members killed businessmen who would not pay money to them, also reporters, politicians, bank owners and other opposed to them. The new criminal class of Russia took on a more Westernized and businesslike approach to organised crime as the more code-of-honor based Vory faded into extinction.

By 1994 Russia's then interior minister, Mikhail Yegorov, stated that the number of organised crime groups in the former Soviet Union had grown from 785 during Gorbachev's reign to 5,500. By 1996 this estimate had grown to 8,000 groups, each with memberships of between 50 and 1,000. The government in Moscow estimated that the Russian mafia controlled 40% of private business and 60% of state-owned companies. Since then, the groups have only increased their influence and power and have expanded across Russia, throughout the former Soviet Union and across the world, operating in over 60 countries, including the US.

Today it is estimated that there are around 6,000 mafia groups in Russia, employing directly or indirectly an estimated three million people. These groups form a state within a state with politicians, army officers, businessmen and policemen on their payroll. Around 200 of the groups are global conglomerates, with estimates of criminal proceeds generated in excess of US\$10bio. The basic business of these groups in Russia is extortion. It has been estimated that nearly 80% of business in Russia pay off the Mafia and sometimes up to 30% of those businesses income goes to the mafia. A prime example, comes from Canadian entrepreneur Doug Steele who owns a well known Moscow nightclub called The Hungry Duck who estimated that he had paid out over US\$1mio in pay-offs to police, officials and the mafia. Mr Steele, who has already survived one kidnapping attempt, said "You have to grease the palm or you won't be in business. "If it was not for the mafia there would not be an economy. They are a major driving force behind what goes on here." The Russian Mafia is also involved in illegal smuggling, particularly Oil and Gas, human trafficking, drug trafficking, smuggling of weapons and nuclear material.

The Russian Mafia is very active internationally and co-operates extensively with other non-Russian organised criminal gangs. According to a Stratfor Global Intelligence report published on 14 November 2007, the US law enforcement has established links between Russian organised crime in the US and La Cosa Nostra. The two groups appear to be cooperating in such ventures as gambling, prostitution, fraud and extortion. The Russian Mafia is responsible for vice operations from Miami to Tokyo to the Persian Gulf, and it is also deeply tied with [Turkish Mafia](#) and Israeli organised crime, most of which came from Russia. Additionally, Russian organised crime groups reportedly have been involved in such enterprises as drug trafficking, money laundering and counterfeiting with several other international organised crime groups, including the [Sicilian Mafia](#), the [Camorra](#), the Japanese

[Yakuza](#), Chinese [Triads](#) and [Colombian Drug Cartels](#). Connections with Latin American Drug Cartels allowed the Russian Mafia to import cocaine into the country.

Russian Mafia gangs are typically called "bratvas", "bratva" meaning "brotherhood" in Russian. While there may be thousands of mafia groups in Russia only a handful are large enough to maintain a serious threat. The biggest and most well known and feared gangs are the Dolgoruadnanskaya Izmaylovskaya; Orekhovskaya Gang and the Solntsevskaya in Moscow the Tambov Syndicate in St Petersburg and Obshina from Chechen.

Solntsevskaya Bratva - Moscow, Russia

This Gang is named after the south west Moscow suburb of Solntsevo from which it originated and has around 5,000 members. Its leader is believed to be Sergei Mikhailov, known as Mikhas, who learned his criminal trade in the Siberian labour camps and who was for a time held by the authorities in Switzerland, but he was let go after several witnesses were shot or blown up and the evidence could not be brought forward. The gang is made up of smaller clans, two of which, the Ostankino and Lubertsy clans are significant players in Moscow. From its base in Moscow, they run rackets in extortion, drug trafficking, car theft, stolen art, money laundering, contract killings, arms dealing, trading nuclear material, prostitution and oil deals.

Tambov Syndicate - St Petersburg, Russia

The Tambov Syndicate is believed to have been formed in 1988 by Vladimir Kumarin and Valery Ledovskikh, both of whom came from Tambov Oblast. In the gang's early period members were recruited almost exclusively from the area of Tambov and formed a protection racket. The group has been involved in various inter gang conflicts, and has suffered in-fighting between its own subdivisions. In the course of such violence Kumarin was subjected to an assassination attempt, loosing an arm but escaping with his life in 1994. The Tambov syndicate is thought to wield significant political power, with members allegedly having gained seats in the State Duma and Saint Petersburg Legislative Assembly. The Tambov syndicate is now led by Vladimir Gavrilenkov.

Semion Mogilevich - Russia

By the mid-1990s it was believed that the Jewish born "Don" Semion Mogilevich had become the "boss of all bosses" of most Russian Mafia Bratvas and described by the FBI as "one of the most dangerous men in the world. Simon Mogilevich is widely seen as the most important figure in the Russian Mafia, most closely associated with the Solntsevskaya Bratva.

Ciscaucasus / North Caucasus

Ciscaucasus/the North Caucasus is the northern part of the Caucasus region between the Black and Caspian Seas and within European Russia, together with the Southern Caucasus also known as Transcaucasus, making up the Caucasus Region.

The North Caucasus, unlike their Southern neighbors are part of the Russian Federation, made up of Russian Republics, consisting of Krasnodar Krai, Stavropol Krai, and the constituent republics, approximately from west to east: Republic of Adygea, Karachay-Cherkessia, Kabardino-Balkaria, North Ossetia-Alania, Ingushetia, Dagestan and Chechnya, also known by separatists as the Chechen Republic of Ichkeria and the region that has been the focus of most trouble and where two wars have been fought.

Whilst Chechnya and these other regions boast a primarily Muslim population, the populace has demonstrated little allegiance to radical Islam, though there is much support for separatist movements many of which have been lead by those with Radical Islamic intent.

These separatist groups were very active during the wars in the Chechen republic from 1994-96 and 1999-09, with some still active today, with acts of reprisals for government actions in the territory, as well as separate acts of terrorism, particularly in Russia, in Moscow and in other large Russian cities and with particular concerns ahead of the Winter Olympics in Sochi in Russia to be held in February 2014

The current threat comes from the Caucasus Emirate, a radical Islamist nationalist organisation formed in 2007 by Doku Umarov after he resigned from his position as President of the Republic of Ichkeria (the self-proclaimed secessionist government of Chechnya) and acting as an umbrella group for radical Islamic secessionist groups in the region.

The group aims to have an independent Caucasus Emirate ruled under Sharia and to aid in waging global jihad. The Caucasus Emirate openly declared their assistance to the global jihadi movement in 2009 at a meeting in Chechnya with the group's top leaders

The Republic of Chechnya

The First Chechen War broke out in 1994. As the Soviet Union disintegrated Chechen separatists declared independence in 1991, forming the Chechen Republic of Ichkeria under President Dudayev. From 1994 Russian forces sought to re-establish control but after 2 years of fighting they withdrew from the region and a ceasefire was agreed. Dudayev was succeeded by Maskhadov, the former Army Chief, who was credited by many with the Chechen victory. Still, with the economy destroyed, and nearly 40% of Chechens displaced and with Chechen warlords still in charge of their own militia's, this time of so called peace and independence became notorious for organised crime, and mayhem. One of the main warlords was Shamil Basayev, who during the First Chechen War made a name for himself and the units under his control. Basayev promoted a much more fundamentalist form of Islam which created a split in the Chechen separatist movement, but which lead President Maskhadov to introduce Islamic Sharia Law and Sharia Courts in 1999.

In 1998 Shamil Basayev, together with Saudi born commander Ibn al-Khattab established the Islamic International Peacekeeping Brigade with members comprised of nationalistic, ethnic Chechen fighters as well as a contingent of Arabs and other foreign fighters dedicated to the creation of an independent Islamic republic in the Russian Republic of Chechnya. Around the same time Arbi Barayev formed the Special Purpose Islamic Regiment with the same goals, forging links between these and other like minded groups. Both groups were later to merge or come together under the umbrella of the Riyad us-Saliheyn Martyrs' Brigade.

Both Basayev and Al-Khattab had visited Afghanistan previously, before 1995, touring and then undergoing training in Afghan fighter training camps, developing close ties to Al-Qaeda. In 1999, new emissaries of Basayev and Al-Khattab traveled to bin Laden's home base in the Afghan province of Kandahar, where bin Laden agreed to provide substantial military assistance and financial aid, including by making arrangements to send to Chechnya several hundred fighters to fight against Russian troops and perpetrate acts of terrorism. Later that year, bin Laden sent substantial amounts of money to Basayev, Al-Khattab and Barayev, which was to be used exclusively for training gunmen, recruiting mercenaries and buying ammunition.

It was also at this time that the first Islamic militants began entering Chechnya to take up the 'cause' for the establishment of an Islamic State in the North Caucasus. These 'Mujahideen' offered connections to terrorist groups and financiers beyond Russia's borders.

In the summer of 1999, Basayev and Ibn Al-Khattab and their Islamic International Peacekeeping Brigade attempted to spread war to the neighboring republic of Dagestan. They also in 1999 attacked at the heart of Russia by killing 130 and injuring 150 in a series of Moscow apartment bombings. Both actions were condemned by President Maskhadov. In response on 1st October, 1999, then Russian Prime Minister, Vladimir Putin, sent Russian forces back into Chechnya, declaring the Chechen leadership as illegitimate and setting off the bloodthirsty Second Chechen War. The actions of Putin, who promised a quick and decisive victory in Chechnya would see him propelled to the Russian Presidency soon afterwards, though a decisive victory was elusive and the war would take 10 years.

President Maskhadov returned to his role as a main commander of Chechen forces along with Shamil Basayev, Ibn Al-Khattab and others, fighting a rearguard action and forming an insurgency following Russian capture of the capital Grozny in 2000.

Whilst there have been many separatist insurgent groups involved in the second Chechen War the following are probably the most important and responsible for most of the most infamous terrorist attacks. These are the Islamic International Peacekeeping Brigade and the Special Purpose Islamic Regiment which later merged to form the Riyad us-Saliheyn Martyrs' Brigade, which has since been succeeded by the Caucuses Emirate.

Following the end of the Second Chechen War in 2009 the Russian government has sought to invest in the Northern Caucasus in an attempt to stem the violence through increasing prosperity in what is one of the poorer regions of Russia. It should be noted that this process had been attempted in Chechnya by politically and economically supporting the 'puppet regime' of President Ramzan Kadyrov. Kadyrov, a former member of a separatist militia himself, is the son of the former President, Akhmad Kadyrov who was assassinated in 2004 by members of the Islamic International Peacekeeping Brigade. He became President in 2007 at the age of 31. Chechnya has been provided with significant funding to bolster his regime, though there have been concerns about the level of corruption and human rights abuses carried out under his regime.

The Islamic International Peacekeeping Brigade

The Islamic International Peacekeeping Brigade (IIPB) was founded by Chechen Separatist Commander Shamil Basayev and Saudi born commander Ibn al-Khattab in 1998. Distinct from some other Chechen resistance groups, the IIPB main objective was not only the creation of an independent Chechen state, but one that would be governed by Islamic fundamentalist Sharia law. In addition to local fighters, the IIPB was bolstered by Arab Mujahideen, brought in from nearby Ingushetia, Ossetia, Georgia, and Azerbaijan, but also from further afield including from Afghanistan, where the IIPB had links with bin Laden and his Al-Qaeda network, which furnished financial, operational, and military support and elsewhere in the Middle East.

The IIPB has been credited with effectively starting the second Chechen War in 1999, with the 1999 apartment bombings in Moscow killing 130 and injuring 150. Explosives had been placed in a rented room in the building. The explosion was one of four similar attacks on apartment bombings in a period of 12 days: the others killed an additional 62, 92 and 17 bringing a total of 301 fatalities for the four attacks. The most infamous attacks would come later with involvement in the 2002 seizure of the Dubrovka Theater in Moscow, alongside other groups the Special Purpose Islamic Regiment and the Riyad us-Saliheyn Martyrs' Brigade. The groups took more than 900 hostages, whom they threatened to kill if the Russian Government did not meet their demands of a complete withdrawal of Russian security forces from Chechnya and the recognition of an independent Chechen state. The standoff ended three days later, when Russian Special Forces troops raided the building, killing all the terrorists involved, but also over 150 civilian hostages were also killed as a result of the operation.

Whilst Ibn al-Khattab was eventually killed in 2002, when a Dagestani messenger hired by the Russian FSB, delivered a poisoned letter to him, he was succeeded by his deputy-commander, Abu al-Walid, however he too was killed in action in 2004, just two years after assuming command of the group. Undeterred by the loss of its two most influential leaders, the Islamic International Peacekeeping Brigade merging into and being succeeded by the Riyad us-Saliheyn Martyrs' Brigade are still regarded as a significant security threat in the region by Moscow.

Special Purpose Islamic Regiment - Chechnya

The Special Purpose Islamic Regiment (SPIR) was formed by Arbi Barayev on or around 1998, with the objective of the formation of an independent Chechen state, forging alliances with other prominent Chechen

resistance organisations as well as foreign Islamic groups. Barayev's was killed in 2001, but was succeeded by his nephew, Movsar Suleimanov, who changed his last name to Barayev in emulation of his uncle, and who played a role in SPIR's most infamous attack which came in 2002, being one of three terrorist groups affiliated with the Chechen insurgency that furnished personnel to carry out the seizure of the Dubrovka Theatre in Moscow, together with the IIPB and the Riyad us-Saliheyn Martyrs' Brigade. Following Barayev (the nephew's) death, in the raid by Russian forces in the Moscow Theatre, the group has been lead by many short lived commanders. It is thought that the group eventually merged with the IIPB to form a larger Riyad us-Saliheyn Martyrs' Brigade.

Riyad us-Saliheyn Martyrs' Brigade - Chechnya

The Riyad us-Saliheyn Martyrs Brigade (RSMB) is a terrorist organisation, dedicated to the creation of an independent Islamic republic in Chechnya (and other primarily Muslim parts of Russia such as Dagestan, Kabardino-Balkaria, Ingushetia, Ossetia and Tataria). The group, whose name translates to "requirements for getting into paradise," espouses a radical Islamic doctrine (Wahabbism) and is believed to have strong ties to Al-Qaeda.

Before his death in 2006, Riyad was led by the rebel commander, Shamil Basayev, who together with Ibn al-Khattab established the IIPB and has been responsible for, or involved in, many of the worst terrorist atrocities claimed by Chechen rebel groups. Riyad is believed to be descended from two other Chechen terrorist organisations, the Special Purpose Islamic Regiment (SPIR) and the International Islamic Peacekeeping Brigade (IIPB). It has even been suggested that Riyad is simply the result of the marriage of these two groups. Riyad terrorists have intensified their attacks in recent years, claiming responsibility for some of the worst terrorist incidents in Russia's history.

Whilst they joined their comrades from the IIPB and SPIR in the Moscow 2002 theatre raid, their first major solo attack took place in December 2002, when they attacked and destroyed the headquarters of the pro-Russian Chechen government, killing 72 and injuring 280 people. In August 2003, an attack was carried out on a Russian hospital housing both civilian and military patients. The attack resulted in the deaths of 52, with 72 injured. Further successful attacks, included the assassination of Akhmad Kadyrov, the President of Chechnya, widely considered a puppet of Moscow, who fell victim to a bomb blast that hit the VIP section of the Dynamo football stadium during a World War II memorial victory parade in May 2004. It is also

responsible for the downing of 2 Passenger airlines, a Volga-Avia Express Flight 1303, killing 43 and a Siberia Airlines Flight 1047, killing 46, with both airlines crashing in Russia within minutes of each other flying different routes. The following investigation found that the planes were downed by bombs triggered by two so called "black widow" female Chechen suicide bombers. Shamil Basayev as overall leader of the Chechen terrorist movement and of RSMB claimed the credit, claiming the cost of the aircraft bombings coming to US\$4,000 in total. Also later in September 2004 Chechen terrorists carried out, perhaps their most horrific act, storming the Comintern Street school in Beslan Russia, taking 1,100 hostages into the school gymnasium, killing the male teachers and fathers of pupils instantly. The hostage siege lasted 3 days when Russian security forces stormed the school, leading in all to 366 killed, including 186 children and 783 injured. Still, these major attacks were to be Basayev's last as he was killed in 2006.

The Caucasus Emirate - Chechnya

The Caucasus Emirate is a radical Islamist nationalist organisation formed in October 2007 by Doku Umarov after he resigned from his position as President of the Republic of Ichkeria (the self-proclaimed secessionist government of Chechnya). The group aims to have an independent Caucasus Emirate ruled under Sharia Law and to aid in waging global jihad. The Caucasus Emirate openly declared their assistance to the global jihadi movement in April 2009 at a meeting in Chechnya with the group's top leaders

Both the Russian Federation and the United States have designated the Caucasus Emirate as a terrorist organisation and the UN added the Caucasus Emirate to the list of entities associated with Al-Qaeda.

The Emirate consists of six provinces that report to their respective emirs who report to the Emir of the Caucasus Emirate, Doku Umarov. The six provinces are all located in the North Caucasus: i) Chechnya, ii) Ingushetia and North Ossetia, iii) Nogay Steppe (Northern Krasnodar Krai and Stavropol Krai), iv) Cherkess and Southern Krasnodar Krai, v) Dagestan, and vi) Kabardino-Balkaria and Karachay.

Upon its creation, the Caucasus Emirate also served as the umbrella for other terrorist organisations from the North Caucasus. These organisations include the Yarmuk (Kabardino-Balkaria) Jamaat, Shariat (Dagestan) Jamaat, and Ingush Jamaat, as well as Riyad us-Saliheyn Martyrs' Brigade from Chechnya.

Under Doku Umarov, the Caucasus Emirate and its

affiliates continued with major attacks in 2010 and in 2011. For example in 2010, two stations on the Moscow Metro were targeted, namely Lubyanka and Park Kultury, by two black widow suicide bombers, killing 40 people and injuring over 100 injured. In 2011, a male suicide bomber struck Moscow's Domodedovo Airport, killing 37 people and injuring more than 180. Doku Umarov ordered a halt to attacks on civilian targets during the mass street protests against President Vladimir Putin in the winter of 2011-12. He later reversed that order urging his comrades to "do their utmost to derail" the Sochi Olympics which he described as "satanic dancing on the bones of our ancestors."

Recent attacks have seen a series of terror attacks on buses, trains and airplanes, some carried out by suicide bombers, including an October 2013 black widow suicide bomber who blew herself up on a city bus in Volgograd, killing 6 people and injuring about 30 and another black widow suicide bomber who blew herself up at a railway station in Southern Russia, killing 14 and injuring scores more, heightening concern about terrorism ahead of February's Olympics in the Russian Black Sea resort of Sochi.

Chechen Mafia - Chechnya

The lines of differentiation between the Chechen and the Russian Mafia are often blurred, primarily as a result of the fact that most people of Chechen ethnicity speak Russian and emigrated from states within the Russian Federation. The Chechen Mafia should however be seen as a distinct entity, and one of the largest organised crime syndicates operating in the former Soviet Union. The organisation emerged in 1974, conceived by the Chechen student Khozh-Ahmed Noukhaev during his time in Moscow. By the late 1980s the Chechens had become the most influential of the Moscow gangs and are today believed to exert extensive international influence. The diverse array of criminal activity in which the Chechen Mafia engages is known to include car theft, drug and human trafficking, money laundering, as well as the illegal sale of plutonium. The Chechen Mafia has at times been separated in terms of its classification from other purely criminal enterprises by dint of its perceived political motivations and links to terrorist cells. During the Chechen Wars it was believed that the revenue from its organised crime network was used to arm Chechen terrorists including separatist fighters. However the end objectives motivating the connections between the Chechen Mafia and Chechen terrorists remain disputed. For instance some observers maintain that the Chechen Mafia did not in fact seek an independent Chechen State, but rather aimed to cultivate and maintain instability in the region as a

way of better propagating their drugs trade. The large Muslim population in Chechnya has led to allegations from Russia's government that the Chechen Mafia has strong links with Al-Qaeda, though such assertions may seek to score political points rather than an accurate portrayal of intelligence. Nevertheless similar allegations have been made by Argentinean authorities who are aware of Chechen links with the Arab Muslim population located in the tri-border area between Argentina, Brazil and Paraguay. The strong Chechen Mafia presence in the region is primarily due to the areas functionality as a shipping point for Andean cocaine to Europe. Claims by the London daily Arab paper al-Watan al-Arabi also support a link between the Chechen Mafia and Al-Qaeda, reporting that the Islamic terrorist organisation had succeeded in procuring twenty nuclear devices from Chechen contacts in return for arms, money and heroin

Obshina - Chechnya

The largest Chechen Mafia is the Obshina, who made much of their money from bank robberies, kidnapping and white collar crime as well as interests in cigarette smuggling. Their leader is Nikolay Suleimanov.

Western Europe



In modern times the political borders of Europe were largely defined and viewed through the prism of the cold war and marked through the existence of the Iron Curtain, with the major Western European States on one side and the Soviet block on the other.

Since the falling of the Berlin Wall Europe's borders and divisions have changed increasingly being divided by those within the EU and those outside and to the East.

Western Europe suffers from a number of different threats from organised criminals and from terrorists. Highly organised gangs such as the Italian Mafia operate mainly in Italy but also in Germany, France and, sporadically in the UK. Domestic gangs based in Netherlands, Sweden, France, UK and Spain also operate.

Europe is also a final destination point as well as a cross-roads for other transnational criminal groups. All of these types have been known to work independently of each other, engage in conflict or, co-operate with each other. Consequently classification is difficult. From the west Colombian cartels are still the main importers of cocaine helped by gangs such as the Italian Mafia and Galician groups in Spain who co-operate in distribution to the whole of Europe.

From the south, Nigerian Gangs are active in trafficking drugs as well as being active in fraud. From the east, Triad groups with communities in the UK, Italy, Austria, Belgium/Netherlands and Portugal are involved in drugs human trafficking illegal gambling and prostitution as well as Russian Mafia gangs involved in all manner of criminal activities across Europe.

The phrase is used loosely to describe gangs from all over Eastern and Central Europe. Gangs from Russia, Poland, Czechoslovakia, Rumania and former Yugoslavia are active in: Spain, Germany, France, Italy, Austria, UK the Netherlands and Sweden. Their main activities are drugs, human trafficking (including prostitution) and the export of stolen cars. For more details see Eastern Europe above. These are hugely profitable enterprises and are also money laundering machines. National organised crime gangs often provide the 'entre' for transnational or foreign groups.

As far as terrorism is concerned, many of the traditional threats within Europe's borders have receded, from anti capitalist and other red groups disappearing, to secessionist and nationalist groups largely giving up violence. The threat that causes most concern is that from Islamic terrorism and in particular from so called Al-Qaeda inspired groups, living in Europe itself.

European Union Designated Terrorist Organisations

The EU³⁹ has designated groups and entities in addition to incorporating the UN designated terrorist lists as follows: Abu Nidal Organisation, Al-Aqsa Martyrs' Brigade; Babbar Khalsa; Communist Party of the Philippines, including New People's Army (NPA), Gamma al-Islamiyya; Great Islamic Eastern Warriors Front; Hamas, including Hamas-Izz al-Din al-Qassam; Hezbollah External Security Organisation; Hofstad Network; Holy Land Foundation for Relief and Development; International Sikh Youth Federation; Khalistan Zindabad Force; Kurdistan Workers' Party (PKK); Liberation Tigers of Tamil Eelam (LTTE); National Liberation Army (ELN); Palestinian Islamic Jihad (PIJ); Popular Front for the Liberation of Palestine (PFLP); Popular Front for the Liberation of Palestine – General Command; (FARC) Revolutionary Armed Forces of Colombia; Revolutionary People's Liberation Army/Front/Party; Shining Path; Al Aqsa Foundation; Kurdish Freedom Falcons.

Abu Hafs al-Masri Brigade

The Abu Hafs al-Masri Brigade may be the name of an active Al-Qaeda cell in Europe or the organisation that oversees Al-Qaeda's European operations. Of course, the Brigade may exist in name only as well. Named for infamous Al-Qaeda terrorist Mohammed Atef aka Abu Hafs, the leader of the 9/11 Attacks on America, Abu Hafs al-Masri Brigade is known only through statements published through the London Arabic language daily al Quds al Arabi. Through this publication, the group has claimed responsibility for several large terrorist strikes, including the July London bombings, the 2004 Madrid train bombings, and the massive blackouts that occurred in North America in the summer of 2003. The attacks for which they claim responsibility are generally attributed to Al-Qaeda, or Al-Qaeda-linked groups. Ayman al-Zawahiri, Al-Qaeda's leader following the death of bin Laden, has claimed responsibility for the organisation on more than one occasion. The group appears to be recently formed (as Atef was only killed in late 2001), but it may reflect only a name-change in memory of Atef for a pre-existing off-shoot or operational division of Al-Qaeda. Doubts of the group's existence stem from the fact that several of their claims are clearly false. The 2003 blackouts, for example, were caused by technical errors. The Abu Hafs group, however, referred to the incident as one of its "operations" - "Operation Quick Lightning in the Land of the Tyrant of This Generation." The Abu Hafs al-Masri Brigade is most likely either a subset of Al-Qaeda or a copy-cat group that has

joined its jihad against the west. Its size and membership are unclear, as is its access to the Al-Qaeda leadership, resources, and network.

Baader-Meinhof Group / Red Army Faction - Germany

Founded in the late 1960s, the Baader-Meinhof Group, otherwise known as the Red Army Faction (RAF), was a violent leftist organisation responsible for several decades of urban terrorism in the Federal Republic of Germany. Originating in capitalist West Germany these communist revolutionaries attacked symbols of capitalist authority, including American targets, public buildings, and notable German industrialists, charging that West Germany's post-war government was as repressive as Hitler's Nazi regime.

Members embraced a blend of anti-capitalist and anarchist beliefs, protesting both the Vietnam War and the occupation of Palestine, whilst also demonstrating its solidarity with other contemporary high profile left-wing movements across the globe.

Though the group referred to itself as the Rote Armee Fraktion, or Red Army Faction (RAF), after the Japanese Red Army (JRA), in an attempt to delegitimise the organisation the media dubbed it the "Baader-Meinhoff Group". On its inception the group constituted a single small cell made up of Andreas Baader, his girlfriend Gudrun Ensslin and two others. This small cell was responsible for the bombing of two Frankfurt department stores in 1968. After being arrested, released, re-arrested and having finally escaped Baader and other prominent group members, including left-wing journalist Ulrike Meinhof, left Germany to train in Jordanian terrorist camps. These camps were run by the Popular Front for the Liberation of Palestine (PFLP) from whom the RAF received small arms training and lessons in terrorist tactics.

On their return to Germany the group perpetrated several bombings that were then described in heroic fashion by journalist Meinhof. Rather surprisingly, in its early years the RAF commanded considerable support and indeed admiration. This esteem arose predominantly as a result of the initial imagery attached to its most prominent founding members. Ulrike Meinhof was a well known figure in the German media, renowned for her radical politics, while Andreas Baader projected the image of a debonair rebel. At first glance therefore this group of urban guerrillas, emerging from a German youth struggling to forge for itself a stable identity in the post-war, post-Nazi era, was somewhat fashionable. Their moment in the sun was short-lived however, and with opinion quickly turning against them the RAF soon became described as an example of

protest taken "too far". By 1972 the groups leading trio: Baader, Ensslin and Meinhof had been captured, leaving a vacuum in which a "second generation" of RAF militants rose. These militants were more committed to the liberation of their idolised leaders than the initiation of the socialist revolution that had been previously sought. Under this new generation of insurgents the RAF focussed almost exclusively on assassinations and kidnappings. However in 1976 Meinhof died in her cell, a fatality recorded as suicide, but which provoked rumours of her execution by security forces. A year later in 1977, just days after the RAF hijacked a Lufthansa plane in an attempt to free their remaining leaders, both Baader and Ensslin were also discovered dead in their cells. Again the deaths were attributed to suicide once it became apparent that RAF exploits would be unable to secure their freedom. Unsurprisingly such explanations raised further suspicions of government authorised executions. The seizure of the Lufthansa plane in 1977 also proved to be the organisation's swan song in terms of daring raids, conducting only intermittent kidnappings and assassinations in the 1980s and early 1990s. After 5 years of almost complete inactivity the RAF formally announced that it had disbanded as an organisation.

Dutch Gangs - Netherlands

The Netherlands occupies a prime position to exploit the international drugs trade; centrally located in Europe it also stands alone as an island of cannabis toleration amidst a sea of law enforcement. Due to the localised nature of cannabis production in Holland, the trade is not controlled by any large organisation, thereby limiting the influence of organised crime groups in what the Dutch deem to be a 'soft drug'. The Dutch organised crime families are traditionally known as the Penose, and in general their groups are loosely organised around individual projects. This is not true of all Dutch crime groups however, and some do form longstanding networks. For instance, two such organised syndicates, Delta Organisation and the 'Octopus Syndicate', rose to prominence in the 1990s, and though little information is publicly available concerning their current status, it is widely believed that organised sections of the Dutch underworld continue to function today.

Bruinsma drug gang - Netherlands

The Bruinsma gang was headed by the infamous Klaas Bruinsma, a man who has in his death gone on to achieve iconic status amongst much of the Dutch population and is even now sported on t-shirts emblazoned with the words 'R.I.P. Bruinsma'. Klaas' work was primarily restricted to the trading and trafficking of drugs, however as is to be expected with underworld commerce, the organisation's work often

involved more violent outlets with assassinations commonly a factor in organisational restructuring and dispute settling. Perhaps the most eye-catching atrocity committed by the group was the grotesque retribution exacted against André Brillman, a body guard accused of stealing. Brillman was dismembered while still alive, to be later concealed in a concrete container and sent to the bottom of the Waal River. Klaas Brunisma did not only deal in drugs, but expanded his trade into the gambling industry, forcing almost every coffee shop in Amsterdam to stock his slot machines. Prostitution was also a string that Brunisma later added to his entrepreneurial bow, adding the famous luxury brothel Yab Yum to his portfolio. The criminal career of Brunisma came to a final end in June 1991 following a quarrel with Martin Hoogland at Amsterdam's Hilton Hotel. Hoogland was a former policeman turned mafia hit-man who it is believed had been contracted to kill Brunisma and so set out to quarrel with the Dutch mafia boss. Following the quarrel Brunisma was shot outside the hotel at 4am, and Hoogland himself perished in March 2004 after an attack by unidentified individuals.

Willem Holleeder gang - Netherlands

Holleeder is a Dutch criminal who rocketed into the public eye with the kidnapping of the Heineken heir Freddy Heineken. This attention grabbing stunt was carried out by Holleeder and his gang, who demanded and received a ransom of NLG35mio (€16mio) from the lager brewing dynasty. The gang did not however escape with the proceeds,

The Hofstad Network - Netherlands

The Hofstad Network is an Islamist terrorist organisation of mostly young Dutch Muslims of mainly North African ancestry. The name "Hofstad" was originally the codename the Dutch secret service used for the network and leaked to the media. The network is said to have links to networks in Spain and Belgium. The group is influenced by the ideology of Takfir wal-Hijra. Redouan al-Issar, also known as "The Syrian" is the suspected spiritual leader of the group. Most media attention is attracted by Mohammed Bouyeri, sentenced to life imprisonment for murdering Dutch film director Theo van Gogh and by Samir Azzouz, suspected of planning terrorist attacks on the Dutch parliament and several strategic targets such as the national airport and a nuclear reactor. The group is also suspected of planning to kill several members of government and parliament.

Communist Combatant Cells - Belgium

The Cellules Communistes Combattantes (CCC; Communist Combatant Cells) was a Belgian terrorist organisation committed to a Communist ideology. The cells were active for less than two years in the mid-

1980s; primarily engaged in bombings within Belgium's borders. While the group was based in Belgium, their targets and goals were predominantly international. CCC attacked perceived enemies of communism, specifically NATO, US and other international businesses and the Federation of Belgian Enterprises.

Original Gangsters - Sweden

The Original Gangsters is an organisation operating in Sweden, originally made up mainly of individuals of an Assyrian/Syriac ethnic background. Its organisational and operational base is in the Swedish city of Gothenburg, and the gang is led by Denho Acar. The group's name is said to have been taken from the lyrics of rapper Ice-T. In 2007 Acar claimed the organisation had 100 all male members, with 30 of those forming an inner circle. Membership is signified by a tattoo depicting the letters OG in the centre of the sun. The gang is known for its violent feuding with other organised crime groups such as the Naserligan, with whom the members of the Original Gangsters engaged in a gun fight outside an unlicensed casino in Gothenburg and various other frays. Conflict has also existed between the Original Gangsters and another gang, the X-Team.

Uppsala Mafia - Sweden

The Uppsala mafia was headed by Stefan Eriksson and operated from Uppsala, Sweden. The group worked behind the legal front of the company Cannon Debt Collectors, collecting debts through threats and violence. The group also attempted to defraud the Swedish bank Giro Central, an offence for which Eriksson and Peter Uf were tried and found guilty. Securing witnesses was however a difficult task for the prosecution as a result of intimidation by the Uppsala Mafia. The lead witness survived two bomb attacks during the course of the trial.

Black Cobra - Denmark

The gang came into existence in 2000 in Roskilde, Denmark, and now numbers approximately 100 individuals. The group operates in a loose network coordinated by strong leadership figures, and members are thought to be involved in drug trafficking, extortion and murder. Individuals associated with the group commonly sport a black and white shirt embossed with the icon of a raised cobra. The gang also exerts control over a distinct youth sub-set known as the Black Scorpions.

Special Focus 19 ETA / Euskadi Ta Askatasuna (ETA) - Spain



ETA or Euskadi Ta Askatasuna (meaning Basque Homeland and Freedom) is an armed Basque nationalist and separatist organisation. Founded in 1959 the movement evolved from a group promoting traditional Basque culture

to a paramilitary group with the goal of gaining independence for the Greater Basque Country. The group is proscribed as a terrorist organisation by the Spanish and French authorities, as well as the EU as a whole and the US. ETA declared ceasefires in 1989, 1996, 1998 and 2006, but subsequently restarted killing. However, in 2011, ETA declared a "permanent, general and verifiable" ceasefire with the expressed aim of ending its campaign.

ETA's motto is Bietan jarrai ("Keep up on both"), referring to the two figures in its motif; a snake (representing politics) wrapped around an axe (representing armed struggle). Since 1968, ETA has been blamed for killing 829 individuals, injuring thousands and conducting dozens of kidnappings. More than 700 members of the organisation are imprisoned in Spain, France, and other countries. ETA organised itself through establishing an overall committee representing numerous functions and responsibilities. These include: logistics, politics, international relations with fraternal organisations, military operations, reserves, prisoner support, expropriation, information, recruitment, negotiation and treasury. The political wing of ETA called Batasuna (formerly known as Euskal Herritarrok and "Herri Batasuna"), is banned in Spain. It pursues the same political goals as ETA and does not condemn ETA's use of violence. It generally receives 8 to 15% of the vote in the Basque Autonomous Community. New successor parties were formed in order to sidestep the prohibition of their participation in the political process, however these organisations were themselves soon outlawed for their failure to condemn violence.

On 5 September 2010, ETA declared a new ceasefire. A spokesperson announced the organisation wished to use "peaceful, democratic means" to achieve its aims, though it was not specified whether the ceasefire was

considered permanent by the group. The announcement was met with a mixed reaction; Basque nationalist politicians responded positively, and said that the Spanish and international governments should do the same, while the Spanish interior counselor of Basque, Rodolfo Ares, said that the commitment did not go far enough. He said that he considered ETA's statement "absolutely insufficient" because it did not commit to a complete termination of what Ares considered "terrorist activity" by the group. On 10 January 2011, ETA declared that their September 2010 ceasefire would be permanent and verifiable by international observers.

ETA was founded by young nationalists, beginning in 1952 as a student discussion group at the University of Deusto in Bilbao. This group broke away from the youth movement affiliated with the Basque Nationalist Party (PNV), disagreeing with the PNV's rejection of violent tactics and advocating a Basque resistance movement using direct action. In an era littered with national liberation movements the Basque movement represented another example of an area that had become conscious of itself as distinct and sought to establish its own nationhood. In their platform, ETA declared that Basque nationality is defined by the Basque language; this was in contrast to the PNV's definition of Basque nationality in terms of ethnicity. Also at odds with the explicit Catholicism of the PNV, ETA defined itself as "a confessional"—meaning ETA does not recognise a special state religion—although it used Catholic doctrine to elaborate its social programme. ETA called for socialism and for "independence for Euskadi, compatible with European federalism".

ETA's first confirmed killing occurred on 7 June 1968, when Guardia Civil, José Pardines Arcay was shot dead when he tried to halt ETA member Txabi Etxebarrieta during the course of a routine road check. Etxebarrieta was chased down and killed as he tried to flee. This led to retaliation in the form of the first planned ETA assassination, that of Melitón Manzanas, chief of the secret police in San Sebastián and associated with a long record of tortures inflicted on detainees in his custody.

The most significant assassination performed by ETA during General Franco's dictatorship was Operación Ogro, the December 1973 bomb assassination in Madrid of Admiral Luis Carrero Blanco, Franco's chosen successor and president of the government (a position roughly equivalent to being prime minister). The assassination had been planned for months and was executed by placing a bomb in the sewer below the street where Carrero Blanco's car passed every day. The bomb blew up beneath the politician's car and threw it three floors into the air and over the top of a nearby

building onto a balcony in a nearby courtyard. This assassination was not condemned by the opposition.

After Franco's death, during the Spanish transition to democracy, ETA split into two separate organisations: one faction became ETA political-military or ETA(pm), and another ETA military or ETA(m). Both ETA(m) and ETA(pm) refused offers of amnesty and instead continued to intensify their violent struggle. The years 1978, 79, and 80 were to prove ETA's most deadly, with 68, 76, and 98 fatalities respectively. In the 1980s, ETA (pm) accepted the Spanish government's offer of individual pardons to all ETA prisoners who publicly renounced the use of violence, even those who had committed violent crimes. However ETA (m) refused to relinquish their violent tactics and continued the armed struggle.

During the 1980s a "dirty war" ensued by means of the Grupos Antiterroristas de Liberación (GAL; "Antiterrorist Liberation Groups"), a paramilitary patriotic group which billed themselves as counter-terrorists. The GAL was active between 1983 and 1987, committing assassinations, kidnappings and torture, not only of ETA members but of civilians supposedly related to the group. Predictably some of these persecuted collaborators turned out to have no real connections to ETA. At least 27 people were murdered in GAL operations. The activities of GAL represented a continuation of similar dirty war actions by death squads, actively supported by members of Spanish security forces and secret services, using names such as Batallón Vasco Español that operated from 1976 to 1982. They were responsible for the killing of about 48 people and as a consequence, the group's attacks since have generally been dubbed state terrorism. ETA performed their first car bomb assassination in Madrid in September 1985. In 1995 an unsuccessful ETA car bombing was directed against José María Aznar, a conservative politician and leader of then-opposition party, Partido Popular (PP). Aznar later went on to win the general election and served for two terms. The group also attempted to assassinate King Juan Carlos of Spain in Bilbao, however the plot was foiled by Spanish police in 1997. On 10 July 1997 ETA kidnapped PP council member Miguel Ángel Blanco in the Basque town of Ermua, threatening to assassinate him unless the Spanish government met ETA's demand for all of its imprisoned members to be returned to prisons in the Basque Country within two days. This demand was rejected and after three days Blanco was found shot dead. In response more than six million people took to the streets to demand his liberation and to protest his murder once news emerged that Blanco had been shot. Massive demonstrations occurred as much in the Basque

regions as elsewhere in Spain, with crowds chanting cries of "Assassins" and "Basques yes, ETA no". This response came to be known as the "Spirit of Ermua".

While public outrage did not stop the lethal attacks, it did however result in a steady erosion of support for the ETA movement. The groups increasing radicalisation, along with Spain's growing familiarity with democracy (the transition from dictatorship to democracy in 1975 became an increasingly distant memory as time passed) also contributed to the decline in ETA support. In the 1998 220 221[TAD2], Basque parliament elections, Batasuna, polled 17.7% of the votes, a figure that by 2001 had fallen to 10%. Moreover by 1999, in the Basque Country, 64% rejected ETA totally, 13% identified themselves as former ETA sympathisers (mainly during the Franco dictatorship) who no longer supported the group. Another 10% agreed with ETA's ends, but not their means. 3% said that their attitude towards ETA was mainly one of fear, 3% expressed indifference and 3% were undecided or did not answer. About 3% gave ETA "justified, with criticism" support (supporting the group but criticising some of their actions) and only 1% gave ETA total support. Even within Batasuna voters, at least 48% rejected ETA's violence. The 11 September 2001 attacks also dealt a hard blow to ETA, owing to the toughening of "antiterrorist" measures, the increase in international police coordination, and the end of the toleration some countries had, up until then, extended to ETA.

ETA was initially blamed for the 2004 Madrid bombings by the outgoing government of José María Aznar, and large sections of the press. However, the group denied responsibility and Islamic fundamentalists were eventually identified as responsible. It was possibly the government's attempts to link ETA to these bombings that affected its popularity in the elections being held only days later. From 2006 onwards ETA has declared a "truce" on numerous occasions, however on 10 January 2011 ETA declared that the ceasefire would be permanent and verifiable by international observers.

In 2007 Spanish police estimated ETA's budget requirements and resources to be approximately €2mio annually. Although ETA used robbery as a means of financing its activities in its early days, it has since been accused both of arms trafficking and of benefiting economically from its political counterpart Batasuna. Extortion remains ETA's main source of funds and is dubbed a "revolutionary tax". Demands are made of business owners in the Basque Country in particular, as well as other areas of Spain, often accompanied by threats against them or their families. Occasionally some French Basques have also been threatened in this

manner, such as footballer Xabi Alonso from whom ETA demanded 'revolutionary tax' in 2000 for playing under the "colours of an enemy state". According to French judiciary sources, ETA takes in an estimated €900,000 a year in this manner.

Kidnapping provides another source of revenue, allowing ETA to leverage large sums of money from targets by way of ransom. These kidnappings are also often used as a punishment for failing to pay the "revolutionary tax", and to try to force the government to free ETA's prisoners under the threat of killing the kidnapped. A further ETA speciality is the art of robbery, commonly seizing weapons, explosives, machines used to manufacture license plates, and vehicles. Those unfortunate enough to be robbed of their vehicles are usually tied and abandoned in an isolated place to allow those who assaulted them to escape. Speculation surrounds ETA's international links, if indeed any do exist. Colombian Vice President Francisco Santos has claimed that FARC (an insurgency group native to Colombia) have attempted to forge connection with the Basque group. According to a report published by the Federal Research Division (Library of Congress) in 2002 ETA has been involved in both weapons and illegal narcotics trafficking in Europe. The Italian author and mafia specialist Roberto Saviano also points to a relationship between ETA and criminal groups, in particular the Italian Mafia. Saviano asserts that ETA traffics cocaine received from its FARC contacts, which it then trades for weapons from the mafia. Following a judicial investigation, it was reported that FARC and ETA held meetings in Colombia, exchanging information about combat tactics and methods of activating explosives through mobile phones. The two organisations were said to have met at least three times. One of the meetings at a FARC camp in 2003 involved two ETA representatives and two FARC leaders and lasted a week. FARC also offered to hide ETA fugitives while requesting anti-aircraft missiles, as well as asking for ETA to supply medical experts who could work at FARC prison camps for more than a year. In addition, and more controversially, FARC also asked ETA to stage attacks and kidnappings on its behalf.

A further international connection maintained by ETA is that with the Provisional Irish Republican Army (IRA); the two groups have both, at times, characterized their struggles as parallel. Links between the two groups go back to at least March 1974 when ETA purchased Strela 2 surface-to-air missiles from the IRA and in 2001 unsuccessfully attempted to shoot down a jet carrying the Spanish Prime Minister, Jose Maria Aznar. ETA has also had links with other militant left-wing movements

in Europe and in other places throughout the world. As a result some ex-militants have received political asylum in Latin American countries, such as Mexico and Venezuela.

France

France is one of the most modern countries in the world and is a leader among European nations as a founder member of the EU, as a permanent member of the UN Security Council, NATO, the G-8, and the G-20. France has suffered from terrorism, both Nationalist and religious in connection with asserting sovereignty over the Island of Corsica in the Mediterranean and due to its Colonial past in North and Central Africa. France's financial and commercial relations, especially with Francophone former colonies, make it an attractive venue for money laundering. Public corruption, drugs trafficking, human trafficking, smuggling, and other crimes associated with organised crime generate illicit proceeds. France continues to be a major destination and transhipment point for drugs trafficking. Most of the illicit drugs in France are produced in other areas of the world. The vast majority of cannabis products in France originates in Morocco, and cocaine available in France is produced in, and trafficked to France from South American countries. The majority of the heroin entering France is produced in Afghanistan and Pakistan.

Current threats against French interests include in particular Mali, and Mali's neighbours in the Sahel and in North Africa.

French Designated Terrorist Organisations

France has designated the following as terrorist organisations:⁴⁰ Accolta Nazionale Corsa; Action Committee of Winegrowers; Action Directe; Action Front for the Liberation of the Baltic Countries; Affiche Rouge; Al-Qaeda; Anti-Armenian Organisation; Anti-Terrorist Liberation Group; Arab Revolutionary Front; Armata Corsa; Armata di Liberazione Nazionale; Army of the Corsican People; Autonomous Intervention Collective Against the Zionist Presence in France; Breton Revolutionary Army (ARB); Charles Martel Group; Clandestini; Clandestini Corsi; Clandestini Ribelli; Committee for Liquidation of Computers (CLODO); Committee of Coordination; Committee of Solidarity with Arab and Middle East Political Prisoners (CSPPA); Corsican Patriotic Front (FPC); Corsican Revolutionary Armed Forces (FARC); de Fes; Francs Tireurs (Mavericks); Fronte di Liberazione Nazionale di Corsica (FLNC); Gazetirak; Gora Euskadi Askatuta; Gracchus Babeuf; Group Bakunin Gdansk

Paris Guatemala Salvador; International Revolutionary Action Group (GARI); Iparretarak (IK); Irrintzi; Masada, Action and Defense Movement; Meinhof-Puig-Antich Group; Moroccan Islamic Combatant Group; Mujahideen-e-Khalq (MeK); National Front for the Liberation of Kurdistan; New Armenian Resistance (NAR); Ninth of June Organisation; Orly Organisation; Palestinian Resistance; Raúl Sendic International Brigade; Resistenza Corsa; Spanish Basque Battalion; Spanish National Action; Takfir wa Hijra; Third of October Group; Totally Anti-War Group (ATAG); Vitalunismo; Youth Action Group

Corsican Mafia (see also National Liberation Front of Corsica) - Corsica, France

One of the most powerful organised crime groups operating in France, the Corsican Mafia hails from the French island of Corsica. Its theatres of operation are not however restricted to France, extending into numerous African and Latin American territories. Within what is known as the Corsican mafia are various distinct gangs such as the Brise de Mer, the Valinco gang, the Venzolasca gang and the Mob of Marseille. The international influence of Corsican mafia groups is argued to stem from the Corsican diaspora; a community of immigrants that spread across the globe and established itself in disparate host nations. This produced Corsican crime figures in Africa, Asia, and even two Venezuelan presidents. Financial sources are from drug trafficking, arms trafficking, human trafficking, prostitution, extortion, money laundering, contract killing, legal gambling establishments.

Corsican Patriotic Front (FPC) - Corsica, France

Founded in the summer of 1999, the Corsican Patriotic Front (FPC) was a nationalist terrorist organisation that sought to preserve the culture and language of the Corsican people and create an independent Corsica. The FPC emerged several days after a clandestine meeting was held by the Corsican National Liberation Front-Historical Wing (FLNC), in which the group rejected Paris' September 1999 call for Corsicans to renounce violence. FPC membership was a relatively loose affair and consisted of militants from other Corsican nationalist terrorist groups as well as Corsican terrorists that acted alone. In an attempt to achieve their objectives, the FPC engaged in small-scale bombings of various business, private, and government targets in Corsica. On the night of September 30th, 1999, the FPC claimed responsibility for six attacks and three other failed attempts. A post office, the holiday home of a 'mainlander,' a local bank branch, a Treasury building, and an electric company office were among the locations targeted by the FPC. The FPC claimed that the attacks were conducted as a result of French

Prime Minister Jospin's 'contempt' towards the Corsican people and culture. In December 1999, the Corsican National Liberation Front (FLNC) issued a general truce to the French government, and the FPC agreed to cease hostilities soon thereafter. However, in April, the FPC issued a statement declaring their frustration with what they perceived to be a lack of effort on the part of the French government to resolve the French-Corsican impasse. Though two attacks in the summer of 2000 were claimed by the FPC, a unilateral truce was issued in August of the same year by the group's leadership. Since then, there has been no mention of the group, and it appears that they are currently inactive. Still, anti-French violence committed by Corsican nationalist groups is expected to continue until a lasting agreement is accepted by both sides.

Traction Avant Gang/Gang des Traction Avant - France

This was a criminal gang based in the Pigalle quarter of Paris, originally made up of surviving members of the Carlingue militia. The Carlingue militia was a mixture of ex-police officers and criminals that had joined the French Resistance to German occupation during World War II. The group's name was derived from their favourite vehicle, the Citroën 11 Traction Avant, which they commonly used in hold ups. The now defunct gang boasted a relatively high profile in its day, counting among its ranks the likes of Pierre Loutrel, France's first "public enemy number one", and the successor to this illustrious title Emile Buisson. This notable public image also inspired the writings of such authors as Alphonse Boudard, Roger Borniche, as well as films by Jean-Luc Godard, Jacques Deray and Claude Lelouch.

Hornec Gang - France

Formed and led by three brothers from the Horne family, this group succeeded crime boss Claude Genova following his assassination in 1994 and is one of the most influential criminal organisations in the Parisian area. Members are most commonly recruited from the ghetto areas of Montreuil, and a large proportion of these young men are of gypsy or Maghrebian ethnic origin. In terms of criminal occupation, the group began with hold-ups, later investing the revenue in night clubs, prostitution bars and real estate. The gang's power is believed to have peaked in the 1990s and early 2000s, diminishing with the arrest of several key members in 2006.

Mad Jacky Gang - France

This criminal organisation is led by Jacques Imbert, also known as "Jacky Le Mat", which translates as Jacky the madman in Provencal. Imbert first rose to prominence in the 1960s, forging an iconic "Godfather" image.

Prior to this ascendancy in the criminal underworld, he had spent time in prison for assault, as well as serving in the French army. Imbert was discharged however on the grounds that his temperament was wholly incompatible with military regulation. In subsequent years Imbert spent time as a member of the Bande de Trois Canards, a group involved in hold-ups, racketeering, and burglaries. It was during this period that Imbert became noted for his self-control and determination, as well as forging relationships with other future gang leaders such as Tony Zampa. The Bande de Trois Canards disbanded in the mid-1960s following the assassination of its then leader, Antoine Guerini. It is likely that this deadly assault came from within the gang itself, with many suspecting Imbert. Imbert himself sustained an assassination attempt in 1977 at the hands of his former comrade Tony Zampa's gang. Receiving multiple bullet wounds (22 bullet fragments were removed from his body), Imbert suffered the paralysis of his right arm. In an act of retribution 11 of Zampa's men were gunned down. Police however failed to pin convincing evidence against Imbert demonstrating his involvement in the killings, and after six months he was released without charge. Police efforts to implicate Imbert in a Russian mafia scheme to establish an illegal cigarette factory in Marseille met with similar failure, Imbert having his 2004 conviction overturned on appeal a year later. Successful conviction of Imbert did however come in 2006 when Imbert was sentenced to 4 years imprisonment for his part in extorting money from Parisian businessmen in the 1990s. To gain a flavour of Imbert's criminal career one might watch the film 22 Bullets, in which Imbert is played by the actor Jean Reno.

Action Directe - France

Action directe was set up in 1977 by two other groups, GARI (Groupes d'Action Révolutionnaire Internationalistes, revolutionary internationalist action groups) and NAPAP (Noyaux Armés pour l'Autonomie Populaire, Armed Core Groups for Popular Autonomy), as the "military-political co-ordination of the autonomous movement". In 1979, it was transformed into an "urban guerrilla organisation" and carried out violent attacks under the banner of "anti-imperialism" and "proletarian defence." The group was banned by the French government in 1984. In August 1985, Action Directe allied itself with the German Red Army Faction. By 1987 however with the leaders arrested, and sentenced to life imprisonment the group's terrorist activities came to an end.

Revolutionary Organisation 17 November - Greece

The Revolutionary Organisation, "17 November" took its name from the date of a 1973 student protest

against the military dictatorship of Greece, though 17N's campaign started after the end of the military and during the succeeding democratic period. 17N believed the democratic government of Greece needed to be replaced espousing a Marxist-Leninist as well as anti-American, anti-Turkey, anti-NATO, anti-EU, anti-Greek establishment, anti-colonial, and anti-capitalist position. 17N was effectively combatted following mass arrests.

Revolutionary Struggle (RS) - Greece

Designated as a Foreign Terrorist Organisation on 18 May 2009, Revolutionary Struggle (RS) is a radical leftist group with Marxist ideology that has conducted attacks against both Greek and US targets in Greece. RS emerged in 2003 following the arrests of members of the Greek leftist groups 17 November.

RS first gained notoriety when it claimed responsibility for the 5 September 2003 bombings at the Athens Courthouse during the trials of 17 November members. From 2004 to 2006, RS claimed responsibility for a number of improvised explosive device (IED) attacks, including a March 2004 attack outside of a Citibank office in Athens. RS claimed responsibility for the 12 January 2007 rocket propelled grenade (RPG) attack on the US Embassy in Athens, which resulted in damage to the building. In 2009, RS increased the number and sophistication of its attacks on police, financial institutions, and other targets. RS bombed a Citibank branch in Athens in March 2009, but failed in its vehicle-borne IED attack in February 2009 against the Citibank headquarters building in Athens. In September 2009, RS claimed responsibility for a car bomb attack on the Athens Stock Exchange, which caused widespread damage and injured a passerby. In 2010, the Greek Government made significant strides in curtailing RS's terrorist activities.

On 10 April Greek police arrested six suspected RS members, including purported leadership figure Nikos Maziotis. In addition to the arrests, the Greek raid resulted in the seizure of a RPG launcher, possibly the one used against the US Embassy in Athens in January 2007. The six, plus two other suspected RS members, face charges for arms offenses, causing explosions, and multiple counts of attempted homicide. Their trial started in December 2011, and if found guilty, the suspects face up to 25 years in prison.

Conspiracy of Fire Nuclei - Greece

The group is a radical anarchist organisation based in Greece. The group emerged in 2008 with a wave of fire bombings against luxury car dealerships and banks and since continued its attacks including bombing.

Cyprus

A former British colony, Cyprus became independent in 1960 following years of resistance to British rule. Tensions between the Greek Cypriot majority and the Turkish Cypriot minority came to a head in December 1963, and by 1974 following intervention first from Greece and then Turkey, the island was split and remains divided. The island entered the EU in 2004. In 2008, the leaders of the two communities began discussions under UN auspices aimed at reuniting the divided island. The talks are ongoing.

Cyprus has attempted to develop itself as a regional financial center, but has suffered recently with a financial crises and a bailout from the EU rescuing the Island.

The biggest threats for money laundering in Cyprus are primarily from domestic and international financial crime. There are over 240,000 international business companies (IBCs) registered in Cyprus, many of which belong to non-residents, and many of which are believed to be owned by Russian and other Eastern European residents.

Holy See (Vatican City)

The Holy See is a unique Sovereign State, based in the Vatican City, in the centre of Rome, only 0.44 square kilometers in size, home and the supreme body of government of the Catholic Church. Whilst not a member of the EU, it nevertheless is a participating member of the Euro, with Vatican Euro's minted and available in the Vatican City. The population of Vatican City, around 800, consists almost entirely of priests (Holy See officials) and members of religious orders, led of course by the Pope of the day, currently Pope Francis.

The Institute for Works of Religion (IOR) whilst not a Bank, performs functions similar to that of a bank, but also of a State Treasury, and it is commonly referred to as the "Vatican Bank." Unlike a normal bank, the IOR does not loan money, and IOR accounts do not collect interest; nor does the IOR make a profit for shareholders or owners. Rather, the IOR acts as a clearinghouse for Vatican accounts, moving funds coming into the Catholic Church mainly from the 18 million visitors each year to the Vatican and from legacies gifted or bequeathed to the church to pay Catholic Church expenditures such as the clergy salaries and expenses as well as for grants and church projects.

There is no private enterprise permitted in the Vatican

City and so there is no market for illicit or smuggled goods in Vatican City, nor any form of illicit activity.

Whilst recognising the unique nature of the Holy See, but also recognising the need to shoulder appropriate responsibilities as a Sovereign State, and responding to concerns the Vatican has, since 2012, begun to accede to relevant international instruments such as the [1988 UN Drug Convention](#), the [UN International Convention for the Suppression of the Financing of Terrorism](#) and the [UN Convention against Transnational Organised Crime](#) and to implement money laundering laws and regulations and independent institutions to oversee and investigate crimes including financial crimes including corruption.

Italy

Home to the Romans and centre of the Holy Roman Empire, Italy, nevertheless became a nation-state only relatively speaking in modern times, in 1861 when the regional states were united together with Sardinia and Sicily. An era of parliamentary government came to a close in the early 1920s when Benito Mussolini established a Fascist dictatorship and fought alongside his ally Nazi Germany leading to Italy's defeat in World War II. A democratic republic replaced the monarchy in 1946, as well as later membership of NATO and the EU.

Italy's long coastline and developed economy entices tens of thousands of illegal immigrants from southeastern Europe and northern Africa, as well as offering ample opportunities for transshipment of Latin American cocaine and Southwest Asian heroin entering the European market. Italy is also home to the infamous Mafia. Earlier in the 1970s it was also struggling with domestic terrorism from Communist groups including the [Red Brigades](#).

Red Brigades - Italy

The Red Brigades was a Marxist/Leninist terrorist organisation based in Italy in the 1970s seeking to establish a revolutionary state through armed struggle, and to remove Italy from NATO. The Red Brigades conducted violent acts designed to destabilise the Italian state through acts of sabotage, bank robberies and kidnappings. In 1978 the group kidnapped then Prime Minister [Aldo Moro](#) killing both members of his entourage and later the Prime Minister himself. The group disbanded after splits and became ineffective by the end of the Cold War.

Special Focus 20 Italian Mafia - Italy



Whilst engaging in a broad range of illegal activities, such as drug trafficking, extortion, smuggling and human trafficking, illegal gambling, counterfeiting, political corruption, murder, weapons trafficking the Italian Mafia also get involved in a range of legal business activities, for example construction though they use Political Corruption to secure government funding and favorable opportunities. According to the FBI their worldwide criminal activity could be worth more than US\$100bio annually or equivalent to nearly 3% of Italy's GDP.

The Italian Mafia has evolved over many generations, first in Sicily, and then throughout particularly the Italian south and abroad, through initially emigration into the US. The Sicilian Mafia changed from a group of largely honorable Sicilian men to an organised criminal group in the 1920s.

Between 1925 and 1929, the Italian Fascists made a concerted effort to eliminate the Mafia and whilst this effort was successful in the short term, the Mafia reestablished itself when fascism fell and was given a further boost when the Allied occupation in 1943 turned to local powers for assistance in governing. The Mafia provided support to the Allied invaders working so closely and successfully with the Allies that it was given the responsibility for Sicily after the end of World War II.

Thereafter the Mafia grew across Italy and began to work as a national enterprise, often using the criminal practices established by La Cosa Nostra in the US, graduating from a quasi-feudal independent association to an international criminal syndicate. For more details see the [Italian American Mafia](#) above in this Section 5. The Mafia established deep relations with important Italian Institutions with bribery and kick-backs becoming commonplace. In response to civil opposition in 1982 Italian law enforcement pushed for new powers which culminated in the adoption of the Anti-Mafia Act and a more aggressive approach to tackling the Mafia which continues today which has managed somewhat to constrain the Mafia's activities.

Their criminal activities are though international with members and affiliates in Canada, South America, Australia, and parts of Europe. They are also known to collaborate with other international organised crime groups from all over the world, especially in drug trafficking.

Whilst the Italian Mafia is perhaps best known for its traditional criminal activities such as drug trafficking, extortion and running protection rackets, today's Mafia in Italy, has become much more sophisticated and has diversified its portfolio of criminal activities. Drug dealing, smuggling, kidnap, people trafficking, prostitution rackets, and the bribery of judges and politicians in Italy are all things that the Mafia deals with.

In recent years there have been reports of the younger generation of Mafia leaders in Italy trying to diversify into white collar crime to make more money. Often, the profits of criminal activities carried out by the Italian Mafia are re invested in legitimate business enterprises.

With the economic crisis affecting banks ability to lend, and the need for business to raise money or realise liquidity, the Mafia have profited as desperate businesses are forced to turn to loan sharks demanding crippling rates of interest, businesses sell ailing businesses, shops and restaurants, cheaply.

There are 4 main groups active in Italy as well as elsewhere, including the US, Canada, South America, Australia, and parts of Europe. These are [La Cosa Nostra](#) or the [Sicilian Mafia](#); the [Camorra](#) or [Neapolitan Mafia](#); the ['Ndrangheta](#) or [Calabrian Mafia](#); and the [Sacra Corona Unita](#) or [United Sacred Crown](#) from Puglia.

It is estimated that these four groups have approximately 25,000 members in total, with 250,000 affiliates worldwide. There are more than 3,000 members and affiliates in the US with the majority related to the Sicilian Mafia.

Le Cosa Nostra or Sicilian Mafia (based in Sicily)

The Italian Mafia emerged first in Sicily, as an underground secret society formed in the mid-1800s to unify Sicilian peasants to fight foreign invaders. In Sicily, the word Mafia tends to mean, Manly, particularly in the sense of a swaggering, fearless, courageous person. A member was known as a "Man Of Honor," respected and admired because he protected his family and friends and kept silent about the society even if faced with death.

The Sicilian Mafia changed from a group of largely

honorable Sicilian men to an organised criminal group in the 1920s. The term Mafia is not one that is actually used. The term cosa nostra or 'our thing' is preferred by Sicilian Mafia members. Like all mafia groups in Italy, the Sicilian Mafia operates a code of honour and has a strict hierarchical structure. Recruits to the Mafia are sworn in to the family through secret ceremonies, after which point they become mafia members and are expected to stay so for life.

The Sicilian Mafia specializes in heroin trafficking, political corruption, and military arms trafficking and is also known to engage in arson, frauds, counterfeiting, and other racketeering crimes. It has also been particularly involved in taking advantage of Government building and infrastructure contracts. The Sicilian Mafia is particularly known for its assassinations of high profile figures including police chiefs, judges and politicians.

Today, the Sicilian Mafia has evolved into an international organised crime group. Some experts estimate it is the second largest organisation in Italy. The Sicilian Mafia is most famous to the outside world because of its branch in America which arose out of mass migration from Sicily in the late 19th century, leading to La Cosa Nostra in the US which became a real problem in the 1920s onwards. With an estimated 2,500 Sicilian Mafia affiliates it is the most powerful and most active Italian organised crime group in the US. Following the arrest of the boss of the Sicilian Mafia, Bernardo Provenzano, in 2006, it is thought that Giovanni Matisi may have taken over this role. Today, the whereabouts of Matisi are unknown. According to some reports he is dead, while others maintain that he is hiding out in Agrigento, in the south of Sicily.

Camorra or Neapolitan Mafia (based in Naples)

The Camorra is a Mafia-type criminal organisation that originated in the region of Campania and its capital Naples in Italy. It is one of the most powerful criminal organisations in the world and dates back to the 16th century. The word "Camorra" was first used in 1735, when a royal decree authorized the establishment of eight gambling houses in Naples. The word is almost certainly a blend of "capo" (boss) and a Neapolitan street game, the "morra." The Camorra has more than 100 clans and approximately 7,000 members, making it the largest of the Italian organised crime groups.

The Camorra made a fortune in reconstruction after an earthquake ravaged the Campania region in 1980. Now it specializes in cigarette smuggling, drug trafficking, counterfeiting, but also extortion, alien smuggling, robbery, blackmail, kidnapping, political corruption, and counterfeiting. It is difficult for officials to fight the

problem because the society of Campania has come to tolerate and accept the mobsters. The area is governed by a code of silence or omertà that persists to this day.

The power of the Naples mafia was recently attested to when in 2004 police were literally surrounded and made hostage by a whole neighbourhood when they tried to capture a local leader. Pasquale Scotti is the head of the Camorra. He has been wanted in Italy since 1985 for murder and other crimes, but he has not been apprehended and is still in hiding. Scotti has been described as a smooth and ruthless personality. He is one of the most able of the lieutenants of the historic leader Raffaele Cutolo. In 1990, an international arrest warrant was issued against Pasquale Scotti, and he received in 2005 a life sentence for a series of 26 murders in his absence.

Ndrangheta or Calabrian Mafia (based in Calabria)

The word "Ndrangheta" comes from the Greek meaning courage or loyalty. The Ndrangheta formed in the 1860s when a group of Sicilians was banished from the island by the new unified Italian government. They settled in Calabria and formed small criminal groups.

There are about 160 Ndrangheta cells, which are loosely connected family groups based on blood relationships and marriages with roughly 6,000 members. They specialize in kidnapping and political corruption, but also engage in drug trafficking, murder, bombings, counterfeiting, gambling, frauds, thefts, labour racketeering, loansharking, and alien smuggling. In the US, there are an estimated 100-200 members and associates, primarily in New York and Florida.

Sacra Corona Unita or United Sacred Crown (based in the Puglia region)

The Sacra Corona Unita became known only in the late 1980s and like other groups started as a prison gang. As its members were released, they settled in the Puglia region in Italy and continued to grow and form links with other Mafia groups. The Sacra Corona Unita is headquartered in Brindisi, located in the southeastern region of Puglia. The Sacra Corona Unita consists of about 50 clans with approximately 2,000 members and specializes in smuggling cigarettes, drugs, arms, and people. It is also involved in money laundering, extortion, and political corruption. The organisation collects payoffs from other criminal groups for landing rights on the southeast coast of Italy, a natural gateway for smuggling to and from post-Communist countries like Croatia, Yugoslavia, and Albania.

United Kingdom-Ireland

The UK has played a leading global role in developing parliamentary democracy and in advancing literature and science. At its height in the 19th century, the British Empire stretched over one-fourth of the earth's surface. The first half of the 20th century saw the UK's strength seriously depleted in two world wars and the Irish Republic's withdrawal from the union. The second half witnessed the dismantling of the Empire and the UK rebuilding itself into a modern and prosperous European nation, but also the fallout from the partition of Ireland leading to decades of troubles over Northern Ireland. The UK is one of five permanent members of the UN Security Council and a founding member of NATO and the Commonwealth and a member of the EU.

The UK is a producer of limited amounts of synthetic drugs and a major consumer of Southwest Asian heroin, Latin American cocaine, and synthetic drugs. It is also a centre for money laundering due its large financial center. Ireland is a more a transshipment point for and consumer of hashish from North Africa to the UK and Netherlands and of European-produced synthetic drugs than a major consumer.

United Kingdom list of Terrorist Organisations

The UK lists the following as terrorist Organisations:⁴¹ [17 November Revolutionary Organisation](#); [Abu Nidal Organisation](#); [Abu Sayyaf](#); [Al-Gama'a al-Islamiya](#); [Al Gurabaat](#); [Al Ittihad Al Islamiya](#); [Al-Qaeda](#); [Ansar Al Islam](#); [Ansar Al Sunna](#); [Ansaru](#); [Armed Islamic Group](#); [Asbat Al-Ansar](#); [Babbar Khalsa](#); [Baluchistan Liberation Army](#); [Euskadi Ta Askatasuna](#); [Egyptian Islamic Jihad](#); [Moroccan Islamic Combatant Group](#); [Hamas Izz ad-Din al-Qassam Brigades](#); [Harkat-Ul-Jihad-Ul-Islami](#); [Harkat-ul-Jihad al-Islami](#); [Harakat-Ul-Mujahideen](#)/Alami; and [Jundallah](#); [Harkat-ul-Mujahideen](#); [Hezbollah](#); [Hezbollah External Security Organisation](#); [Indian Mujahideen](#); [International Sikh Youth Federation](#); [Islamic Army of Aden](#); [Islamic Jihad Union](#); [Islamic Movement of Uzbekistan](#); [Jaish e Mohammed](#); [Jammat-ul Mujahideen Bangladesh](#); [Jeemah Islamiyah](#); [Khuddam Ul-Islam](#) and splinter group [Jamaat Ul-Furquan](#); [Kurdistan Workers Party](#); [Lashkar e Tayyaba](#); [Liberation Tigers of Tamil Eelam](#); [Palestinian Islamic Jihad](#); [Shaqqaq](#); [Revolutionary Peoples' Liberation Party - Front Salafist Group for Preaching and Combat](#); [Sipah-E Sahaba Pakistan](#); [Lashkar-e-Jhangvi](#); [Libyan Islamic Fighting Group](#); [Saviour Sect](#); [Tehrik Nefaz-e Shari'at Muhammadi](#); [Kurdistan Freedom Falcons](#).

According to Wensley Clarkson, in his book the "Gangs of Britain" today's UK gangs are streets apart from the old style gang lords of recent history. Still the most notorious gang leaders and criminal gangsters of recent times include the Adams Family, the Arif brothers, Jimmy Moody, Curtis Warren, Luisa Bolivar, Roddy McClean, John "little legs" Lloyd, John "goldfinger" Palmer, Paul Ferris, Andrew Billimore and Josie Daly. The UK's Serious and Organised Crime Agency (SOCA) recently published a list of the UK's most "toxic" criminals, listing 145 so-called criminal bosses (already convicted) regarded as career criminals for involvement in all manner of serious crime, including drug trafficking, fraud, money laundering, involvement in counterfeit currency and property from the proceeds of crime. One of the first on the list is [Terry Adams](#), boss of the [Clerkenwell Syndicate A Team](#).

Saor Eire - Ireland

Saor Eire meaning Free Ireland was an armed, radical Irish Republican organisation composed of Trotskyists and ex-IRA members. Formed in 1967, its leaders came from the Left wing Irish political parties it was intended as an urban guerrilla group. Its leaders believed that the working class was key to the armed struggle. Its sole political statement was the Saor Éire Manifesto published in May 1971. Between 1967 and 1970, Saor Éire carried out a number of bank robberies, the proceeds being used to purchase arms. The group provided arms, training and funding to Nationalists in Northern Ireland after the outbreak of the Troubles in 1969. A raid on two banks in Newry in County Down in March 1969 netted £22,000, the biggest single haul from a robbery in the country at the time. In February 1970 the group took over the village of Rathdrum in County Wicklow, stopping traffic and cutting phone lines, and robbed the local bank. On 3 April 1970, in the course of a bank robbery in Dublin, a police officer, Garda Richard Fallon, was shot and killed. He was the first member of the Irish security forces to die in the Troubles. Saor Éire was officially disbanded in 1975.

The Kray Twins Firm - East London, UK

During the 1950s and 1960s twin brothers "Ronnie" Kray and "Reggie Kray" headed an organised crime syndicate known to many as the Firm. The Firm's power base was established by the Kray twins in London's East end where they extended their assets to include nightclubs. This line of work granted the twins access to London's social elite and in time the brothers themselves became somewhat iconic figures. For many years the Kray brothers functioned unhampered by law enforcement in their criminal enterprises, having bribed and intimidated their way out of many condemning circumstances. In particular being known

for violent retribution provided ample protection from prosecution, with witnesses unwilling to testify against the Firm for fear of condemning themselves to a brutal demise. The Krays apparent stranglehold on the British justice system was not however permanent, for in May of 1969 the infamous duo were arrested by Detective Superintendent 'Nipper' Read. Read led a squad of detectives specially selected for the investigation and prosecution of the Kray twins. With a case built by this specialist team and with the brothers behind bars the fear of reprisals subsided and some witnesses were prepared to provide their testimony. In this manner the Firm's leaders were finally held accountable for their actions, both being sentenced to life imprisonment. Ronnie spending the rest of his life behind bars, as did Reggie apart from 8 weeks compassionate release prior to his death from cancer.

The Clerkenwell Crime Syndicate / the A team - the Adams Family - North London, UK

This gang has repeatedly been linked to around 25 murders and attributed a collective holding of £200mio. Prior to the conviction of two brothers in 1998 and 2007, the belief had begun to circulate the influence of the group was so great as to make them untouchable by law enforcement, bribing and intimidating themselves beyond the reach of the UK's justice system. This criminal organisation was established on the basis of a familial unit in the 1980s by Terry Adams and his brothers Sean (a.k.a Tommy) and Patrick (a.k.a Patsy). A group of Irish Catholic descent, the A-team located its powerbase close to the family home in the Clerkenwell district of Islington, North London. It was here that the brothers first began their criminal careers, intimidating and extorting money from stall holders at local marketplaces. Their criminal activity evolved significantly from these comparatively humble origins, with members of the organisation believed to have a strong presence in drug trafficking, extortion, security fraud, and even the hijacking of gold bullion shipments.

In terms of organisational structure, it is believed that Terry led the outfit, Sean dealt with the groups, Curtis Warren the finances and Patrick provided the enforcement wing. In the 1970s and early 1980s the Adams family were linked to a number of robberies, using high powered motorbikes as getaway vehicles. The proceeds of these crimes were invested in a variety of local cash businesses, such as minicab firms and car washes, later followed by drinking establishments. In 1983, the family joined forces with others, playing a role in the £25mio Brinks Matt robbery at Heathrow Airport, and their share helped solidify their power and influence in North London and for investments in the burgeoning cocaine and cannabis boom, establishing

links with Columbian drug cartels and other trafficking enterprises such as Yardie groups. The revenue produced by this trade was laundered by corrupt specialists and so found its way into legitimate business and property holdings. While the gang had over several years been repeatedly linked to around murders and criminal activity becoming notorious to both the authorities and the media, it wasn't until 1998 and 2007 that following trials for two of the brothers, convictions would be secured. In 1998 Sean "Tommy" Adams was convicted for organising an illegal hashish smuggling operation estimated to be worth £8 million. As a result he received seven years imprisonment, however in order to avoid facing a further five years imprisonment Sean agreed to pay £1mio in fines; a sum provided by his wife who twice came to court carrying a briefcase containing £500, 000. In 2007 Terry Adams was sentenced to seven years imprisonment after pleading guilty to money laundering charges. These charges were brought against Terry Adams following an investigation conducted by the UK's Serious and Organised Crime Agency (SOCA) and as a reflection of the group's importance, SOCA was assisted by the UK's security service MI5. On arrest arts and antiques valued at £500,000 in total were seized, as well as £59,000 in cash concealed in a shoebox in the attic, and £48,000 worth of jewellery was seized from his North London home. No legitimate means of acquiring this money, or that used to purchase the family home could be established. Terry Adams served just over 3 years, around half of his sentence before being released.

The Noonan Gang - Manchester, UK

The Noonan Gang was a family based crime syndicate established by Desmond "Dessie" Noonan and Dominic Noonan in the Manchester area. The family is headed by Dominic Noonan, for whom his brother Desmond functioned as a fixer until his death in March 2005. The fatality occurred just days before the brothers featured as the subject of a tv documentary on national television. Desmond's personal path to crime began in the 1980s as a doorman, where his fighting skills and general appearance soon began to win him respect amongst Manchester's nightclub clientele as well as sections of its criminal underworld. In time Desmond began to place his own security men on club doors and by the late 1980s it was estimated that around 80% of the city's night time security industry was controlled by the Noonan family. Control of the greater part of Manchester's criminal enterprise fell to the Noonan brothers in 1991 with the murder of rival crime boss Anthony "White Tony" Johnson, leader of the Cheetham Hill Gang. Desmond Noonan was charged with this murder, later to be acquitted following a re-trial. As the 1990s came to a close the Noonans had

been connected to 25 murders, numerous robberies including raids on banks, and maintained control of the security industry in several of the UK's most prominent cities.

Thomas McGraw - East London, UK

McGraw's early criminal activity began in the 1980s, a period in which he began to buy his first pubs and nightclubs. Involvement in this industry offered McGraw the opportunity to expand into the suitably matched drugs trade, including the sale of heroin. According to the biography of fellow criminal Paul John Ferris, McGraw's heroin trade was forged from close connections with the police force. In covert trade operations McGraw would receive confiscated drugs from corrupt officers, which he and his associates would then sell to users and other dealers. It is believed by some that McGraw, while undoubtedly heavily involved in organised crime, was also an informant for the Serious Crime Squad and in this way provided himself with a measure of immunity from prosecution. For instance following his arrest for a failed robbery, during which he was apprehended after a short chase in vehicles and on foot, McGraw was released without charge the very next day. In similarly unusual circumstances McGraw was acquitted of a charge of attempted murder after his attack on a police officer in 1978, adding to speculation that he had bought immunity in exchange for information on his associates. In 2002 McGraw also made a miraculous escape from an attempt on his life near his home in the East End. Despite being stabbed several times McGraw's life was saved by a bullet proof jacket he had acquired and happened to be wearing at the time of the attack. Thomas McGraw died in 2007 of a suspected heart attack.

Curtis Warren - Liverpool, UK

Curtis Warren is among the UK's most notorious criminals, leading a drug trafficking and criminal operation from his native Liverpool. As a juvenile Warren had a colourful criminal history, spending two years under supervision at the age of 12 after stealing a car. At 13 he appeared in court for burglary, aged 15 he spent three months in a detention centre, and having reached the age of 18 he was sent to borstal after assaulting a police officer. Warren learnt his trade from his occupation as a nightclub doorman. It was this role that first introduced Warren to the drugs trade, discovering his ability to control the entry of drugs into the clubs for whom he provided security. Warren was therefore effectively able to control drug supply into some of its most profitable marketplaces, and soon made connections dealers.

In the course of his criminal career Warren has been involved in several noteworthy case investigations, where he has managed to avoid a successful prosecution. In 1993 Warren escaped prosecution for the smuggling of vast quantities of Venezuelan cocaine. The drugs were contained in steel boxes, themselves embedded in lead ingots. The first shipments passed successfully through HM Customs and Excise checks, even after officers cut one of the ingots open and came tantalizingly close to a discovery. Once the shipment had made its successful transit, Dutch law enforcement authorities informed HM Customs and Excise of the concealment by Warren, by which time all evidence was untraceable. Nevertheless, by the time a second shipment reached British shores HM Customs and Excise were well prepared, immediately seizing the shipment and arresting Warren, his co-conspirator Charrington and 26 others. During the course of proceedings however it emerged that Charrington was a police informant. While this was deemed to be of little significance by HM Customs who continued in their pursuit of a conviction, the leaning of Charrington's police "handlers" and Conservative MP Tim Devlin resulted in charges against Charrington being dropped, followed soon after by the entire case. Allegedly, on his release Warren is said to have walked past disgruntled HM Customs officers and remarked: "I'm off to spend my £87mio from the first shipment and you can't touch me." Moving to Holland, to escape threats in the UK and to be closer to the centre of his drug trafficking operation, the Dutch authorities were nevertheless watching, and following a raid by Dutch Police, they uncovered three guns, ammunition, hand grenades, crates with 960 CS gas canisters, 400kg (880lb) of cocaine, 1,500kg (3,300lb) of cannabis resin, 60kg (130lb) of heroin, 50kg (110lb) of ecstasy, and NLG400,000 plus US\$600,000 in cash. All told the haul was estimated to value £125mio, and led to Curtis Warren's imprisonment in Holland. Whilst he would still continue to operate his drug trafficking network his lengthy jail term, was further increased following the death of his cell mate during a prison fight.

Cahill Gang - Ireland

The Cahill gang was established by Martin Cahill and his brothers who embarked on a criminal enterprise together from their adolescence onwards. The brothers moved from household burglaries to armed robberies, picking up members as they progressed in the Irish underworld. The most famous heists carried out by the Cahill gang were the theft of IR£2mio in gold from O'Connor's jewellers. Cahill's notoriety as a criminal leader became so great as to earn him the title 'The General' amongst the media. The threat he and his gang posed to public safety and security was also deemed to

be sufficient to warrant the establishment of a dedicated police division tasked with monitoring their movements around the clock. The division was named Tango Squad, and Martin Cahill became Tango-1. Whilst the authorities continued to pursue him and his gang, it was from another direction that would lead to his downfall. In 1984 Cahill was assassinated, shot whilst stationary at a road junction in his car. The identity and affiliation of the murder remain unknown, though speculation was that it was the work of the IRA.

Gilligan Gang - Ireland

The Gilligan gang was formed by John Gilligan in 1993. The group began by illegally trafficking duty free cigarettes into Ireland, before progressing into illicit drugs. In 2001 John Gilligan was himself awarded a 30 year sentence (later reduced to 20 on appeal) for possession of commercial quantities of cannabis resin. In the eyes of the media John Gilligan and his gang are most renowned for their alleged connection to the death of investigative journalist Veronica Guerin. Guerin is thought to have been working on a piece investigating the involvement of John Gilligan in the illicit drugs trade at the time of her death, and her murder led to a large scale investigation involving more than 100 officers. John Gilligan was however acquitted of the murder in 2002, but remained in prison to serve other convictions (for possession of large quantities of cannabis and threatening to kill two police officers).

Foley Gang - Ireland

Martin Foley, commonly known as "the Viper", is one of Ireland's most well known contemporary crime figures, and occupies a prominent position in Dublin's McCormack-Foley crime family. His criminal career began as a drug dealer, later an associate of Martin Cahill, another infamous criminal of Dublin's gangland. Foley's criminal activity has not gone unnoticed by law enforcement and he has received 33 convictions as a result. In 2007 Foley set up a debt collection firm, "Viper Debt Recovery and Repossession Service" and has subsequently been investigated following allegations of intimidation. Foley has also endured many attempts on his life, being shot on five separate occasions, miraculously surviving them all.

Terrorist Groups

A number of armed paramilitary groups are also proscribed because of involvement in the Troubles in Northern Ireland as follows: Continuity Army Council (CAC); Cumann na mBan; Fianna na hÉireann, a name claimed by multiple groups; Irish National Liberation Army (INLA); Irish People's Liberation Organisation (IPLO); Irish Republican Army (IRA), a name claimed by multiple groups; Loyalist Volunteer Force (LVF);

Orange Volunteers; Red Hand Commando; Red Hand Defenders; Soare Éire; Ulster Defence Association (UDA); Ulster Freedom Fighters (UFF); and the Ulster Volunteer Force (UVF).

Irish National Liberation Army - Northern Ireland

In 1972, following a series of politically damaging attacks against civilians, the Official IRA declared a ceasefire and announced its intention to join the political process. The Official IRA, with its leftist ideology, emerged in 1969 following the split of the Irish Republican Army (IRA) into the Official and Provisional factions. Republican dissents, desiring a continuation of the armed struggle against the British presence in Northern Ireland, broke away from the organisation and formed the INLA in 1974. The INLA also known by a number of aliases such as the Catholic Reaction Force (CRF), People's Liberation Army (PLA) and the People's Republican Army (PRA). Members of the INLA have conducted attacks against British security forces, Northern Ireland's police forces, Protestants (civilians and paramilitaries), and rival republicans through the use of bombings, assassinations, and armed attacks. The group's most publicized attack occurred in May 1979 when it claimed responsible for the assassination of Airey Neave, a prominent member of the British Parliament and close political supporter of Margaret Thatcher. Airey Neave was killed by a car bomb shortly before the 1979 election that resulted in the selection of Margaret Thatcher as prime minister. In 1997, three imprisoned members of the INLA assassinated Billy "King Rat" Wright, the Loyalist Volunteer Force (LVF) leader in the Maze prison. The Irish People's Liberation Organisation (IPLO) emerged in 1986 from a split within the INLA from both disaffected and expelled INLA members. It developed a reputation for intra-republican violence and criminality, before being forcibly disbanded by the Provisional Irish Republican Army (IRA) in 1992. In 1998, the INLA declared a ceasefire although it remains opposed to the Good Friday Agreement. Its ceasefire was declared just days after the 1998 Omagh bombing in Northern Ireland. Although the attack was attributed to another republican terrorist group, the Real IRA, the INLA has been implicated as providing supplies for the bombing, including transportation vehicles.

Special Focus 21 Provisional Irish Republican Army - Ireland



The history of the IRA is both complex and fascinating. The movement and the name originated in the armed struggle for Irish independence from British Rule, which was successfully achieved, albeit in part, during the Irish War of

Independence 1919–1921. This conflict led to the signing of the Anglo-Irish Treaty in December 1921 and the creation of the Irish Free State, which held sovereignty over 26 of 32 Irish Counties. The remaining six Counties of Ulster (Donegal excepted) were retained by Britain under first Irish premier W. T. Cosgrave.

The Irish Republican Army (IRA) was at the vanguard of this all Ireland armed struggle for independence, however following a split between those in favour of the Treaty, (an opinion largely formulated on pragmatic grounds, believing that a full defeat of the British in Ulster was not possible) and those determined to continue the struggle for an all Ireland Independence. Those in favour of the Treaty, including many IRA units, formed the nucleus of a new Irish National Army under the new Irish Free State Government, while opponents of the Treaty remained outside the government and were nicknamed the "irregulars". Nevertheless these so called "irregulars" continued to call themselves the IRA. The reasons why some IRA volunteers became regulars and others irregulars were complex, but an important factor was an evaluation of the military situation where no consensus could be reached. Powerful personalities and their conclusions as to the success or failure of the Treaty also played an important role in the allegiances of larger IRA units. For example, whereas Michael Collins, the most celebrated of Irish Republican Soldiers, was in favour of the Treaty, others including Eamon de Valera would be imprisoned for their opposition, inciting others to do the same and eventually leading the cause for full Irish unity.

Public support however was reflected in the victory of the "regulars" in the general elections of 1922 and

1923, but still the country remained divided, with regulars holding most of the new Irish Free State but the irregulars holding much of the south and west of Ireland. Despite having started with a numerical advantage at the outset of the civil war, the irregulars were soon both outnumbered and outgunned; with massive aid from the British bolstering the regulars. The regulars best troops were the Dublin Guard - a unit composed of former IRA men, who became regulars primarily out of personal loyalty to Michael Collins. By 1923, the defeat of the irregulars in the civil war was assured. It controlled no territory and its guerrilla campaign had little public support. Eamon de Valera wrote "Further sacrifice of life would now be vain and continuance of the struggle in arms unwise in the national interest and prejudicial to the future of our cause. Military victory must be allowed to rest for the moment with those who have destroyed the Republic. Other means must be sought to safeguard the nation's right."

Significantly however, the civil war had not been brought to an end by any kind of agreement between the two sides. The IRA of the post-civil war era would never accept the Free State as a legitimate Irish government and would continue to oppose its existence and perpetuate the struggle against British rule in the 6 counties. In the elections of 1932 de Valera's Fianna Fail party won the election and despite fears the results would not be respected Cosgrave's party peacefully gave up power and instructed the police and armed forces to obey the new government. Initially, de Valera's Fianna Fail government was friendly towards the IRA, legalising the organisation and freeing all their prisoners who had been interned. However by 1935 this relationship had turned to enmity on both sides. The IRA accused Fianna Fail of "selling out" by not declaring "The Republic" and by tolerating the continued partition of Ireland. In 1936, de Valera banned the IRA. Despite this move, most of the IRA's republican constituency were reconciled to the Free State by De Valera's government, which introduced a republican constitution in 1937, abolishing the Oath of Allegiance to the British monarchy and introducing an elected President as head of state. The document also included a territorial claim to Northern Ireland. By the late 1930s at the latest, most Irish people disagreed with the residual Irish Republican Army's claims that it remained the legitimate 'army of the Republic'. In Northern Ireland, the IRA's main role was to try to defend the Catholic community during periodic outbreaks of sectarian rioting.

During the Second World War, the IRA leadership hoped for support from Germany to strike against

Britain during the war, and IRA leadership travelled to Germany in 1940 to canvass for arms and to support an invasion plan for Northern Ireland. Up until the 1960s the IRA operated the border campaign which involved various IRA units carrying out a range of military operations, from direct attacks on security installations to disruptive actions against infrastructure. The campaign initially received significant support from the south, however internment without trial, introduced first in Northern Ireland and then in the Republic of Ireland, curtailed IRA operations and ultimately broke the group's morale. The campaign was on the whole a failure. It petered out in the late 1950s, and was officially ended in February 1962.

In the 1960s the IRA split on ideological grounds with its then leadership espousing left wing marxist ideas of class that precluded the defence of republican catholic working class groups in northern island from the predations of nationalist and protestant working class communities. This led to a break away by the "Provisional IRA," from the now "Official IRA" who retained a traditional republican view and saw themselves as defenders of the Republican Catholic minority in Northern Ireland. The Provisional IRA then embarked on a thirty year armed campaign known as "the Troubles" against the British presence in Northern Ireland, which claimed 1707 lives. In 1997 it announced a ceasefire that effectively marked the end of its campaign. In 2005 it formally announced the end of the campaign and destroyed much of its weaponry under international supervision. The movement's political wing, Provisional Sinn Fein, is now a growing electoral force in both Northern Ireland and the Republic. The Official IRA mounted their own armed campaign up to 1972, when they called a ceasefire, though some activities continued until 1979.

IRA Financial Needs

The IRA were in many ways as much like an organised criminal gang as a terrorist organisation, with involvement in many forms of lucrative criminal activity, including, kidnapping for ransom, armed robbery, extortion and drug trafficking, in addition to donations or contributions from either states, organisations or individuals. Whilst the level of finance available to a terrorist organisation will fluctuate and whilst a group can be sustained on low budgets, a well financed terrorist organisation will have access to more sophisticated weapons, enough funding to carry out planned operations. Perhaps most importantly insufficient finances can lead to the curtailing of political ambitions, precluding the proper function of a political wing such as Sinn Fein. Conducting a terrorist campaign requires human resources (in terms

of individuals prepared to take the risk of planting a bomb or aiming and firing a weapon) but it also requires material resources: bombs, rifles or other forms of weaponry. The IRA have at times, employed significant weaponry despite the difficulty of obtaining such hardware on the open market. Surface-to-air missiles, Russian-made rocket-propelled grenade ('RPG') launchers, assault rifles and machine-guns from the US, Libya and Russia, as well as many smaller arms including shotguns and pistols have all been used by the IRA. The IRA is also believed to have procured many heavy machine-guns, a number of which are believed to have been supplied by Libya. Far cheaper, but sometimes just as effective, are the homemade munitions which the IRA has increasingly manufactured. IRA 'engineers' have demonstrated their ability to make homemade mortar bombing equipment and homemade bombs. These bombs have been made from commercial and home-made explosives, employing their own radio-controlled detonation devices, or 'sleeper' devices, enabling bomb detonation after a long period. The IRA has also used 'vehicle' bombs with cars, trucks, buses, or vans. The attack of course makes the news but financing the operation itself is usually much less than the cost of planning and preparation, including, training and procuring weapons, transport and other equipment. Transport costs for example are incurred in many ways: this includes everything from petrol for the car used in a robbery or for transportation of weapons to an operational area - to some of the more sophisticated operations which include the incursion of PIRA terrorists into another country. Therefore transport costs may well involve the purchase of a train, bus, or even airplane ticket, as well as the food and accommodation costs necessary to sustain members in the operational area for perhaps up to a week or sometimes longer. Radio equipment is another commodity of vital importance in allowing the PIRA to monitor security force movements, and has evolved considerably since the early 1970s.

Terrorist campaigns need of course weapons, but of far greater importance are the personnel to use these destructive tools. If these individuals are already known to security forces organisational support is required for them to exist within clandestine lives, and a permanent cadre of volunteers needs to be maintained for operational needs. Various types of safe houses have to be maintained, both to secure men on the run, but also to offer active terrorists opportunities to relax and unwind away from the threat of the security services. Cost in this respect can involve payment of money to some safe house owners who provide meals or lodgings to IRA members, or who provide a temporary resting place for periods ranging literally from minutes to

weeks. Other safe house owners who perhaps stored weaponry, or parts of weaponry for the PIRA would be paid not only to ensure their discretion, but also as recompense for the considerable risk they ran in aiding the organisation. As a result a large proportion of those who provided safe houses for the PIRA were widows or unmarried mothers in need of additional income. A further major concern for the PIRA leadership is the welfare of prisoners' relatives, the support of men 'on the run' and their families, as well as men released after serving prison sentences and who consequently had minimal employment prospects. An issue of some debate is the extent to which IRA Volunteers are salaried. With informed estimates of 400-500 IRA members, weekly payouts could certainly add up. In one case a senior figure was said to receive a sum close to £6,000 at one Christmas during the 1994-96 ceasefire. The costs incurred by the IRA's political wing, Sinn Fein, are equally extensive. For the IRA legitimate political representation by Sinn Fein has become an increasingly important aspect of the overall Republican movement in recent years. Financial sustenance is needed for everything from the maintenance of premises (from the Sinn Fein Headquarters in 44. Parnell Square, Dublin, and in Belfast, to the Regional offices around the 32 counties, to public meetings in hotels or pubs even in rural areas) and costs incurred during elections.

IRA Financing

Generally speaking, individuals do not join political terrorist organisations for money. In the case of the PIRA, we know that individual members do not live lavish lifestyles. The income generating activities of the IRA remain to this day no different from other terrorist organisations except in scale, although the PIRA probably shows more sophistication and specialization than most. Security sources in Northern Ireland and in the Republic both gather intelligence on the Provisional IRA's 'incidental' activities the purpose of which is to raise funds for the organisation. Source descriptions demonstrate the IRA's involvement in a variety of revenue generating activities, from at least one clear example of 'riding shotgun' (providing an armed escort for payment) on an international drugs shipment, to money laundering schemes in the US, Northern Ireland, and the Republic. The latter involves the purchase of legitimate businesses with illegally obtained funds. Such businesses may then be run as commercial enterprises, yielding 'legitimate' profit which finds its way back to the terrorist organisation. Alternatively the businesses may be exploited using fraudulent or other means to maximize returns and avoid tax, later to be abandoned or sold on once their usefulness has expired. An examination of one such business located in the Republic of Ireland is the focus of one of our case

studies. Legitimately owned businesses have included private security firms, the 'black' taxi cabs in Belfast (one co-operative of over 300 taxis located on the Falls Road is estimated to have had an annual income of about US\$1.32mio - income which is legally reported to the British taxation authorities). They also include at least two known hackney cab services in Dublin, construction firms, shops, restaurants, courier services, guest houses, cars and machinery, pubs which at one time or another have included at least one in Boston in the US, two small pubs in Finglas, several in Dublin, two in Coolock, three in Letterkenny, Co. Donegal, three in Cork (including one Cork hotel), and more small pubs scattered about the country. The 'mini empire' also includes social clubs (with some illegally installed slot machines to augment income from the legal ones), illegal drinking clubs or 'shebeens' and antiques (sometimes having been stolen in the Irish Republic and resold at various markets in Britain). Social welfare fraud is reported as particularly common, and protection rackets and extortion (from pubs and clubs, shops, and business people) are nothing less than a fact of many people's lives in certain areas.

Support groups, such as NORAI (the Northern Aid Committee) and FOSF (Friends of Sinn Fein), the Irish-American fundraising bodies, local collections in pubs and clubs in Ireland and voluntary private donations (including cheques of £100-£150 having been frequently given by businessmen across the 32 counties) are further sources of funds - this last source is one not to be underestimated or obscured by suspicions of more sophisticated forms of raising money such as money laundering. Other activities include income tax frauds involving the use of false tax exemption certificates (on Northern Ireland building sites), the smuggling of grain, livestock (even the smuggling of bovine antibiotics and livestock growth promoters), the pirating of video and audio media, the pirating of computer games, and the theft of cars (along with anything else required for operational duties). Fundraising has even included the sale of contraband cigarette lighters in Belfast, and in the past kidnapping for ransom purposes. One of the best known and certainly widely-reported sources of funds have come from armed robbery (see the Northern Bank Robbery in Part 2, Section 7, Criminal Cases).

This wide array of activities leads to some specialisation of function within the organisation and the need for a Finance Department, with its Director and support staff presently drawing on the experiences of experienced bank managers and at least two accountants. Although estimated, the annual income for the IRA in 1990 was £5mio and in 1996, £10mio. The following specific areas of criminal conduct provide much of the finance required by the IRA; including kidnapping for ransom,

robbery, extortion, drugs and money laundering.

Kidnapping for Ransom

As with robbery, kidnapping for ransom is a traditional method of raising funds for many terrorist organisations around the world. Some groups are more successful than others; the Basque Separatist group ETA (Euzkadi Ta Askatasuna - Basque Homeland and Freedom); has relied considerably on this practice to raise funds. A popular avenue has been the kidnapping of wealthy businessmen or executives of large companies as these targets present the prospect of large ransoms. However, unlike the IRA's successes through other fundraising avenues, the organisation's experiences at kidnapping for ransom did not have such a thoroughly auspicious life-cycle. In October 1979, the IRA kidnapped Ben Dunne from his home in Dublin. A member of the Dunne family, owners of an extensive chain of retail stores in Ireland, he was released five days later in south Armagh, amid 'considerable controversy as to whether or not a ransom was actually paid by the Dunnes to the IRA. It is suspected that the sum of £750,000 may have been paid. The Dunne kidnapping was the first of several such operations undertaken by the IRA, with the kidnapping of Margaret Fennelley, the wife of a Cork bank manager, two months later in December 1979. Then, after a series of abductions in Dublin and Wicklow targeting the families of bank managers, ransom payments were delivered to the IRA before the Gardai could become involved. In the case of Margaret Fennelley and her £60,000 ransom, however, the Gardai actually succeeded in rescuing the woman before the payment could be made.

This was not the case for all kidnappings however as demonstrated when the daughters of two bank managers, were abducted, from Dundalk and Ardee, in Co. Louth just across the border from Co. Armagh in the north, when two ransoms of £50,000 each were delivered before the police could act. One of the most celebrated kidnappings to occur took place on 8 February 1981 when Shergar, the thoroughbred horse and Derby Winner, was taken from stables at the Curragh (near the Irish Army headquarters). Although 'the Shergar affair' (or perhaps more accurately, 'mystery') has never fully been resolved, the horse was apparently put down by his kidnappers when the owning syndicate led by Aga Khan, failed to pay the demanded ransom. There was also some speculation that Shergar's kidnappers could not handle the animal and consequently killed him. Shergar's body has not been found, but interest in the case continues. In April 1996, it was announced that the investigation was to reopen with an examination of forensic evidence to establish a DNA link between the suspected carcass of Shergar and

hair samples from the horse. Thus far, this seems to have proved inconclusive.

In 1983, five IRA members were charged and convicted of the attempted kidnapping of Galen Weston, a multi-millionaire from Canada. Gardai, acting on information supplied to them, simply laid in wait until the PIRA gang arrived at Weston's house in Co. Wicklow. Also, in October 1983, Alma Manima was kidnapped from Greystones, Co. Wicklow. Although Manima was released and a number of local PIRA members were arrested, Coogan noted 'it is not clear what happened to the £60,000 ransom'. Furthermore in 1983, a tragic event was to contribute to the eventual long-term decline of kidnapping for ransom by PIRA active service units. Following the kidnapping of Associated British Foods executive Don Tidey, an Irish soldier and a Garda were both killed as police and army personnel surrounded the PIRA unit and their hostage in Ballinamore, Co. Leitrim, engaging in a fierce shootout. However, if kidnapping was to decrease, the PIRA's involvement in robbery certainly would not.

Robbery

Although it is difficult to quantify the number of PIRA-related robberies in Northern Ireland and the Republic, robbery certainly appears to be one of the PIRA's main 'outwardly' sources of funding, if not the single main source. Such incidents illustrate part of a consistent series of well executed robberies, but it is probably impossible to gauge the total number of robberies for which the PIRA have been responsible over the years, both North and South. For an example of a particularly prominent case see the Northern Bank Robbery in Part 2, Section 7, Criminal Cases below. After a robbery has been committed, the haul can be collected by a person (not necessarily a member of the ASU who committed the robbery) and is sometimes stored locally, for use against local costs. The loot is often passed along a chain to designated individuals, sometimes to be stored in office safes, invested in other operations, or concealed as a result of money laundering techniques.

Extortion

Some of the earliest examples of extortion date back to the PIRA's first attempts at fundraising. The PIRA began in the early 1970s to demand 'protection' money from publicans, local businessmen, shopkeepers and so on in Northern Ireland, through intimidation and in some cases, quite overt threats. Protection would be demanded in a quite straightforward manner. The gang, typically three or four strong, would march into the premises, brandish a weapon and demand money; if the owner did not pay up they might break a few windows or beat him up. This rather heavy-handed practice

appears to have subsided somewhat. The 'greening' of the PIRA with the birth of more covert fundraising activities, including money laundering which appear to have overshadowed overt extortion.

In the North, the establishment of PIRA-controlled security companies has emphasised that to survive any local 'security threats', hiring the right company to control security could be a wise choice. Today, the whole operation has become more sophisticated and gentlemanly. Any contractor or business new to an area controlled by one of the paramilitary organisations was previously approached by representatives of the group concerned, but now the approach is generally made by an apparently legitimate security company. This security company has in fact been established by a terrorist group in order to provide a veneer of legitimacy to what in truth remains a simple protection racket. These new and apparently legitimate sources of funds have been increasingly popular among terrorists in recent years. Another clear example of attempted extortion became evident in 1988, when the Bank of Ireland in the Republic issued the following statement to all of its branches:

"SECURITY ALERT - STAFF BRIEF" The Bank has received a demand for £2mio from a paramilitary group which has identified itself as the Provisional IRA. The demand was accompanied by an unspecified threat against the Bank. We are satisfied that this threat should be taken seriously. The Bank's priority in the face of any threat is the safety of our staff and the public. This priority can only be effectively served by not acceding to demands of this nature. We believe that if we ever acceded to such a demand, we would be placing our staff at greater ultimate risk. The best advice available to us strongly supports this policy. While it is not easy to gauge precisely the substance of any threat received, it would be prudent for all of us to exercise extra vigilance in the weeks ahead and to adhere fully to security procedures in the interests of both staff and public.⁷

Drug Trafficking

Discussion of profiting from drugs by the PIRA raises controversial issues, as do any allegations of PIRA influence on the behaviour of anti-drugs community movements in the south of Ireland. One major form of PIRA community activity has been its involvement in anti-drug activities in inner city areas, and there is no doubt that Sinn Fein has gained political benefit from such involvement in regions including Dublin. PIRA militants were also renowned for keeping Catholic areas of Ulster drug free, regularly kneecapping and intimidating drug dealers. On the other hand, there are enormous financial profits to be made from the

drug trade, and any involvement in the control and distribution of illegal drugs would clearly net the PIRA considerable financial gain. This proved an allure too great for some PIRA members who are reputed to have involved themselves in the international drugs trade, forging links with American criminal organisations. For instance in 1988 a plot to smuggle Bolivian cocaine into the UK by a combined group of IRA and Detroit Mafia was exposed by police after a tip-off. Nevertheless such isolated incidents should be viewed critically, and not taken as representative for the larger organisation as a whole. While a few members more than likely succumbed to the temptation of the drug trade and its profits, the organisation largely eschewed and actively restrained the drugs trade in Ireland. Moreover the IRA emblem was worn falsely by numerous unconnected criminals in order to cultivate credibility, making it equally plausible that the Boston drug traffickers apprehended in 1988 shared with the IRA nothing more than an Irish accent.

Perhaps the most famous of all Robberies in the UK was the heist now known as the Great Train Robbery which took place in 1963, where £2.6mio was stolen from a post office delivery train. While the robbery has commonly been seen as the work of one gang, in truth the group contained two distinct gangs; that of Bruce Reynolds and the South Coast Raiders. In total 16 men are believed to have gathered on the tracks, with leaders Bruce Reynolds and since famed Buster Edwards and Ronnie Biggs members of the gang. Previous criminal exploits undertaken by the men in the gang had focussed on banks and other places known to house large amounts of cash. However as banks became increasingly secure the group began to look elsewhere for high value hauls, focusing on cash in transit as a vulnerable target to exploit. Whilst the robbery was initially a success all known gang members were arrested and imprisoned.⁷

Money Laundering

The IRA is believed to have operated a large scale system of money laundering in order to finance its campaigns. For instance the Daily Telegraph reported in 1992 that investigators had discovered a complicated and advanced system by which IRA members channelled money from Northern Ireland to the London Stock market, and back once more into Northern Ireland where it could be easily accessed by IRA members without detection. In 2005 police also foiled an alleged attempt by the IRA to buy a Bulgarian bank as a front through which it could launder vast amounts of money. The capital required to even contemplate such a purchase demonstrates the financial resources that the IRA network could access. The most prominent case of IRA money laundering

emerged in the 2009 trial of Ted Cunningham, the financial adviser accused of laundering vast sums of money for the group following the [2004 robbery of Northern Bank](#) in Belfast. While Cunningham was found guilty of all 10 counts levelled against him in the original trial, since then the search warrant used by the police to enter Cunningham's house has been found insufficient for the purposes to which it was put, and Cunningham has been released on bail with a re-trial ordered to reconsider the remaining 9 counts against him. Money laundering, with its complex transactions and minimal personal attachment, is by nature a difficult crime to prosecute. Nevertheless the sophistication and size of the IRA and its financial mechanisms has led to its nicknaming as the Rafia.

Continuity IRA - Northern Ireland

The Continuity IRA (CIRA) was designated as a US Foreign Terrorist Organisation on 13 July 2004, the Continuity Irish Republican Army is a terrorist splinter group formed in 1994 as the clandestine armed wing of Republican Sinn Fein; it split from Sinn Fein in 1986. "Continuity" refers to the group's belief that it is carrying on the original Irish Republican Army's (IRA) goal of forcing the British out of Northern Ireland. CIRA cooperates with the larger [Real IRA \(RIRA\)](#).

CIRA has been active in Belfast and the border areas of NI, where it has carried out bombings, assassinations, kidnappings, hijackings, extortion, and robberies. On occasion, it provided advance warning to police of its attacks. Targets have included the British military, NI security forces, and Loyalist paramilitary groups. CIRA did not join the Provisional IRA in the September 2005 decommissioning and remained capable of effective, if sporadic, terrorist attacks. On 21 April 2011, authorities defused an explosive device planted by CIRA near a statue of the Duke of Wellington in Trim, Meath, Ireland. CIRA supported its activities through criminal activities, including smuggling. CIRA may have acquired arms and materiel from the Balkans, in co-operation with the [RIRA](#).

Cumann na Mban - Ireland

The Irish Women's Council is an Irish republican women's paramilitary organisation formed in Dublin, Ireland in 1914 being bound into the struggle for Irish Independence and allied with the IRA. The group has opposed the peace process and has since aligned itself with the [Continuity IRA](#).

Real Irish Republican Army - Northern Ireland

Designated as a US Foreign Terrorist Organisation on 16 May 2001, the Real IRA (RIRA) was formed in 1997 as the clandestine armed wing of the 32 County Sovereignty Movement, a "political pressure group"

dedicated to removing British forces from NI and unifying Ireland. The RIRA has historically sought to disrupt the NI peace process and did not participate in the September 2005 weapons decommissioning. In September 1997, the [32 County Sovereignty Movement](#) opposed Sinn Fein's adoption of the Mitchell principles of democracy and non-violence. Despite internal rifts and calls by some jailed members, including the group's founder Michael "Mickey" McKeitt, for a cease-fire and disbandment, the RIRA has pledged additional violence and continued to conduct attacks. Many RIRA members are former [Provisional Irish Republican Army](#) members who left the organisation after that group renewed its cease-fire in 1997. These members brought a wealth of experience in terrorist tactics and bomb making to the RIRA. Targets have included civilians (most notoriously in the Omagh bombing in August 1998), British security forces, and police in NI. The Independent Monitoring Commission, which was established to oversee the peace process, assessed that RIRA members were likely responsible for the majority of the shootings and assaults that occurred in NI. In October 2011, Lithuanian authorities convicted a RIRA member for attempting to arrange a shipment of weapons to NI in 2008. In 2011, the group was responsible for seven attacks on NI businesses and the Police Service of NI (PSNI) and was suspected of other incidents. In January, May, and October 2011, the RIRA damaged office buildings, government facilities, and banks in improvised explosive device (IED) attacks, and in February authorities defused another IED before it could explode. RIRA attacked PSNI officers investigating a car theft, and officials blamed RIRA for a bomb placed under a police car that killed a Catholic police officer. RIRA conducted two separate attacks. The RIRA is suspected of receiving funds from sympathizers in the US and of attempting to buy weapons from US gun dealers. The RIRA was also reported to have purchased sophisticated weapons from the Balkans and to have occasionally collaborated with the [CIRA](#).

The 32 County Sovereignty Movement - Northern Ireland

The 32 County Sovereignty Movement often abbreviated to 32CSM or 32csm, is an Irish republican political organisation based in Derry. It is not a political party that stands in elections, rather a community pressure group. The 32CSM's objectives are the restoration of Irish national sovereignty via achieving unity among the Irish people, promoting the revolutionary ideals of republicanism and bringing to an end all forms of colonialism and imperialism. The name refers to the 32 counties of Ireland which were created by the Kingdom of Ireland and claimed by the Irish people, the original inhabitants of the island,

through the Irish Republic declared in 1916 and voted overwhelmingly in by a fully franchised electorate in 1919. Due to the partition of Ireland in 1920–22, twenty-six of these counties formed the Irish Free State which became the Republic of Ireland, and the other six in what became Northern Ireland remain part of the United Kingdom. Many of the 32 County Sovereignty Movement's founding members had previously been members of Sinn Féin and they were also involved with a sub-group within Sinn Féin called the "32 County Sovereignty Committee". The 32CSM are often referred to as the 'political wing' of the [Real IRA](#). The organisation was founded in 1997 at a meeting in Dublin by republican activists who were opposed to the direction taken by Sinn Féin and other mainstream republican politicians in the peace process, which would lead to the Belfast Agreement (also known as the Good Friday Agreement) the following year. The same division in the republican movement led to the paramilitary group now known as the [Real IRA](#) breaking away from the [Provisional Irish Republican Army](#) at around the same time. This group is currently considered a foreign terrorist organisation in the United States as the group is considered to be inseparable from the [Real IRA](#), who are designated as a terrorist organisation. In 2001 the US Department of State stated that "evidence provided by both the British and Irish governments and open source materials demonstrate clearly that the individuals who created the [Real IRA](#) also established... [32CSM] to serve as the public face of the [Real IRA](#).... with.... [32CSM] engaging in propaganda and fundraising on behalf of and in collaboration with the [Real IRA](#)".

Ulster Defence Association / Ulster Volunteer Force - Northern Ireland

Numerous groups have formed to counter both the threat from Irish republican terrorist groups as well as seeking to maintain the status of Northern Ireland as part of the UK. These include the two main groups also closely linked being the UDA and the UVF and related and associate groups, the Red Hand Defenders, Red Hand Commandos, the Orange Volunteers and the Loyalist Volunteer Force all of which have been designated as terrorist organisations by the UK government. The UDA is the largest loyalist paramilitary followed by the UVF in Northern Ireland. It was formed in September 1971 and undertook a campaign of almost twenty-four years during "The Troubles". It also used the name Ulster Freedom Fighters (UFF) when it wished to claim responsibility for attacks and, because the two claimed to be separate organisations, the UDA was able to remain legal for over twenty years. The UK outlawed the "UFF" in November 1973 and the UDA itself was classified as a terrorist group on 10 August 1992. The UVF was formed in late 1965 or

early 1966 and named after the Ulster Volunteer Force of 1913. The group's volunteers undertook an armed campaign of almost thirty years during The Troubles. It declared a ceasefire in 1994, although sporadic attacks continued until it officially ended its armed campaign in May 2007. For both the UDA and the UVF and/or their affiliates, robbery has been described as the preferred source of funds, though legitimate business have also provided funds for example, like the [IRA](#), the UVF also operated black taxi services, a scheme believed to have generated £100,000 annually for the organisation, to have been involved in the extortion of legitimate businesses, to a degree involved in organised crime and in some cases implicating in drug dealing. In 2002 the House of Commons Northern Ireland Affairs Committee estimated the UVF's annual running costs at £1–2mio per year, against an annual fundraising capability of £1.5mio. In contrast to the [IRA](#), overseas support for loyalist paramilitaries has been limited, with benefactors mostly in the UK and particularly in Scotland. The UDA and UVF are made up of a number of satellite or affiliate organisations including the Red Hand Commandos, the Red Hand Defenders and the Orange Volunteers and the Loyalist Volunteer Force. The Red Hand Commandos were formed in 1972 and became quickly affiliated with the UVF and was declared illegal in 1973. The RHC waged a paramilitary campaign from 1972 until the loyalist ceasefires of 1994. The Red Hand Commandos should not be confused with the Red Hand Defenders which first emerged in 1998 at the same time as another loyalist paramilitary group, the Orange Volunteers and who are believed to share the same members and are believed to be used by larger loyalist groups like the UDA and UVF to enable members to continue to conduct attacks while their organisations observe ceasefires. The Loyalist Volunteer Force was formed in 1996 as a splinter group from the UVF. The UDA/UVF and many of the affiliate groups declared a ceasefire in 1994 on behalf of all loyalist paramilitary groups. The UDA/ UVF supported the signing of the 1998 Good Friday Agreement and maintained a ceasefire from 1994 until full and final decommissioning in or around 2009. The UVF has killed more people than any other loyalist paramilitary group. According to the University of Ulster's Sutton database, the UVF and RHC was responsible for 481 killings, whilst the UDA/UFF was responsible for 259 killings.

Fianna Eireann - Ireland

The Warriors of Ireland were somewhat akin to the boy scouts movement of Ireland, being established in 1909 but also joining the struggle for Irish Independence. Whilst the group has been disbanded it has essentially been replaced with Sinn Féin Republican Youth.



Section 6 - Terrorist Attacks

Introduction, 509

- Chronology .of the World's Worst Terrorist Attacks over the last 100 Years, 511
- Special Focus 1 - 2001: Attacks on America (9/11), 518
- Special Focus 2 - 2004: Train bombings in Madrid, Spain (3/11), 521
- Special Focus 3 - 2005: London trains & bus bombings (7/7), 524
- Chronology .of the World's Worst Airline attacks by Terrorists, 531
- Special Focus 4 - 1988: Pan Am Flight 103, 534
- Special Focus 5 - 2010: UPS Flight 232 & FedEx Cargo Planes, 537

Introduction

When we think of countries most at risk of terrorist attacks, we usually think of Iraq, Pakistan or Afghanistan. Whilst these countries remain in the top 5 countries at risk, according to a 2011 report from Maplecroft, Somalia is now more at risk than any other country in the world and with the fledgling state of South Sudan also making the top five at number 5. The Top 4 countries are believed to sustain over 75% of world's fatalities from terrorism with terrorist attacks are on the increase globally.

Top 5 at Risk Countries for terrorist attacks		
1	Somalia	Extreme: 1,385
2	Pakistan	Extreme: 2,163
3	Iraq	Extreme: 3,456
4	Afghanistan	Extreme: 3,423
5	South Sudan	Extreme: 211

Source: Maplecroft 2011¹

The latest Terrorism Risk Index (TRI), released by risk analysis and mapping firm Maplecroft, rates 20 countries and territories as 'extreme risk,' with Somalia (1), Pakistan (2), Iraq (3), Afghanistan (4) once again topping the ranking. The 'extreme risk' category also includes: South Sudan (5), Yemen (6), Palestinian Occupied Territories (7), DR Congo (8) Central African Republic (9), Colombia (10), Algeria (11), Thailand (12), Philippines (13), Russia (14), Sudan (15), Iran (16), Burundi (17), India (18), Nigeria (19) and Israel (20).

Looking at the year on year data, Maplecroft's research also reveals that the number of terrorist attacks rose by approximately 15% globally, with 11,954 incidents between April 2010 and March 2011, compared to 10,394 from April 2009 to March 31st 2010. However, there was a decrease in fatalities falling to 13,492 from 14,478.

Significantly the TRI also reveals that the number of terrorist incidents in Afghanistan increased by over 50% over the same period, rising from 2,246 attacks in 2009/10 to 3,470 in 2010/11.

According to the Global Terrorism Database (GTD), an open source event database (insert reference and link) that includes 82,000 domestic and international terrorist attacks since 1970. The GTD shows that Terrorist attacks reached their twentieth century peak in 1992 (with over 5,100 attacks worldwide), but had substantially declined in the years leading up to the 9/11 attacks. In fact, total attacks in 2000 (1,351) were at about the same level as total attacks in 1977 (1,307) and worldwide terrorist attacks through the mid-1970s were

relatively infrequent, with fewer than 1,000 incidents each year. From 1976 to 1979 the frequency of events nearly tripled. The number of terrorist attacks continued to increase until the 1992 peak, with smaller peaks in 1984, at almost 3,500 incidents, and 1989, with over 4,300 events. After the first major peak in 1992, the number of terrorist attacks declined until the end of the twentieth century, before rising steeply to a 10-year high of nearly 3,300 in 2007 – four years after the start of the Iraq war. Still, total attacks in 2007 were 36% lower than total attacks for the 1992 peak. Fatal attacks also declined in the years prior to the 9/11 attacks. In fact, fatal attacks in 2000 (580) were considerably lower than they had been more than two decades earlier, in 1979 (832). In general, the number of fatal attacks clearly followed the pattern of total attacks. Fatal attacks rose above 1,000 per year for the first time in 1980. After hovering close to 1,000 attacks annually for most of the 1980s, they more than doubled between 1985 and 1992. Like total attacks, fatal attacks declined somewhat after 1992, bottoming out in 1998 with 426 attacks and then rising again to a global peak of more than 2,100 fatal attacks in 2007. The peak in 2007 (2,111) was similar to the peak in 1992 (2,178).

Most Frequently attacked Countries by Terrorist attacks		
1	Colombia	6767
2	Peru	6038
3	El Salvador	5330
4	India	4318
5	UK / NI	3762
6	Spain	3165
7	Iraq	3161
8	Turkey	2691
9	Sri Lanka	2611
10	Pakistan	2536
11	Philippines	2490
12	Chile	2287
13	Israel	2140
14	Guatemala	2023
15	Nicaragua	1986
16	South Africa	1921
17	Lebanon	1913
18	Algeria	1650
19	Italy	1487
20	US	1362

Source: Global Terrorism Database since 1970

In short, in the 4 years prior to 9/11 worldwide terrorist attacks and fatal attacks were at their lowest level in 20 years. However, both total and fatal attacks have increased considerably since then so that in 2007 attacks were back to levels they had been at in the mid-1990s and fatal attacks were approaching the peak year of 1992.

The US has long been perceived as being the target of an inordinate number if not a majority of terrorist attacks, though this is in fact not the case, with Colombia taking top spot with the most attacks and Iraq with the most fatalities.

Latin America had the largest number of terrorist attacks of any region of the world throughout the 1980s and the first half of the 1990s. Four Middle Eastern or Persian Gulf countries are in the top 20 (Iraq, Turkey, Israel and Lebanon) and four are in South Asia or Southeast Asia (India, Pakistan, Sri Lanka, Philippines). Western Europe contains three countries in the top 20 (UK/Northern Ireland, Spain and Italy). South Africa and Algeria are the sole countries from Africa in the top 20 most frequently targeted countries.

Most Fatalities by Country from Terrorist Attacks	
Iraq	17,754
Sri Lanka	14,272
India	14,434
Colombia	13,009
Peru	12,496
El Salvador	12,496
Nicaragua	11,324
Algeria	8,545
Philippines	6,304
Pakistan	5,540
Guatemala	5,135
Turkey	4,674
Burundi	4,084
Afghanistan	3,764
US	3,394
Rwanda	3,200
Lebanon	3,093
Russia	3,057
Angola	2,861
UK/NI	2,842

Source: Global Terrorism Database since 1970

Worlds Worst Top 15 attacks by Terrorists (excluding assassinations and pure Airline Attacks, excluding attacks in war zones, for example Afghanistan and Iraq)

Major Fatalities / Terrorist Attacks	
191	2004: Attack on Madrid Trains in Spain by AQ inspired
192	2004: Attack on refugee camp in Uganda by Lord's Resistance Army
202	2002: Bali Bombings in Indonesia by Jemaah Islamiyah
233	1987: Bus attacks in Sri Lanka by Tamil Tigers
238	1997: Attacks in Algeria at Sidi Moussa by GIA
300	1990: Attack at mosques in Sri Lanka by Tamil Tigers
301	1983: Truck bombings of US at French barracks, Beirut, Lebanon by Hezbollah
301	1999: Bombings of apartment buildings in Moscow Russia by Chechen Rebels over 12 days
303	1998: Truck bombings of US embassies in Nairobi, Kenya & Dar es Salaam, Tanzania by Egyptian Islamic Group & Al-Qaeda
317	1993: 15 bombings in Mumbai, India by D-Company
366	2004: School Hostage Crisis, Beslan Russia by Chechen Rebels
477	1978: Cinema Rex Arson Abadan, Iran by Iranian Revolutionaries
780	2009: Attack on city in Nigeria by Boko Haram
865	2008: Christmas attacks in Northern DR Congo by Lord's Resistance Army
2997	2001: Attack on America on 9/11 by Al-Qaeda

Source: Author (excluding attacks in war zones, for example Iraq and Afghanistan and Airline Bombings (see later))

Chronology of the Worlds Worst Terrorist Attacks over the last 100 Years

Over the years Countries at risk have changed though the continuing long standing political and religious conflicts in the Middle East have provided many of the most shocking terrorist attacks. The following is a chronology of perhaps the Worlds worst terrorist attacks causing mass casualties or proving to be important to understand trends and effects. The list includes some major political assassinations and is supplemented by a chronology of Airline Bombings below.

1914: Archduke Franz Ferdinand assassination in Sarajevo by Serbian Nationalist

The assassination of the Archduke and his wife in a car in Sarajevo (the capital of modern day Bosnia-Herzegovina but at the time part of greater Serbia and occupied by the Austro-Hungarians) had terrible repercussions, leading to World War 1. The assassin a Serbian national, with ties to the Serbian Military, was seen by the Austro-Hungarians as a terrorist. In response, Austro-Hungary held the Serbian government complicit in the murder and set in motion the wheels of war which would, in turn, start a chain of events that would, over the course of a just a few weeks, bring the two to conflict, but see Germany support the Austro-Hungarians and in response the French, Russian and British support the Serbians. Over the next four years, the Great War as it would be later called would grow to involve Italy, Japan, the Middle East and the US, among other countries. More than 20 million soldiers died and 21 million more were wounded, while millions of other people fell victim to the influenza epidemic that the war helped to spread. The war left in its wake three ruined imperial dynasties (Germany, Austria-Hungary and Turkey) and through the Communist revolution in Russia led to the downfall of the Tsar.

1920: Wall Street Bombing: US by Galleanists (Italian anarchists) (38)

In the Financial District of New York City, a horse-drawn wagon loaded with dynamite exploded. The blast killed 38 and seriously injured 143, mostly messengers, stenographers, clerks and brokers as its victims. Although the bombing was never entirely solved, investigators and historians think it likely the Wall Street bombing was carried out by Galleanists (Italian anarchists), a group responsible for a series of bombings the previous year. The attack was related to postwar social unrest, labour struggles and anti-capitalist agitation in the US. At that time it was the deadliest act of terrorism on US soil up to that point.

1921: bombing of Bolgارد palace in Bessarabia (modern Moldova) (100)

A bomb was thrown at the Bolgارد palace in Bessarabia (modern day Moldova), killing 100, mostly police and soldiers.

1925: bombing of cathedral in Sophia, Bulgaria by Communist Revolutionaries (160)

A crowded cathedral was bombed in Sophia, Bulgaria, during a funeral for a government official. The bombing, at the Sveta Nedelya Cathedral, was apparently intended to kill the Bulgarian king who nonetheless survived. The premier and war minister were among those killed. Bulgarian authorities concluded that the bombing was conducted by Communists supported by the Soviet Union, and many Communists were arrested and executed (reportedly at least 6,000 and 400, respectively) for the bombing.

1933: First 2 Airline Attacks (15) and (7)

It wasn't until 1933 that the first 2 Aeroplanes were destroyed intentionally first by fire and then by a bomb and is thought to be the first proven acts of air terror in the history of commercial aviation. Imperial Airways flight over Belgium crashing probably after a fire started by a passenger attempting to commit suicide, killing all 15 aboard. This is thought to be the first act of sabotage on a commercial airliner. This was followed by United Airlines Boeing 247 which was destroyed by a bomb, crashing near Indiana, USA, killing 7, thought to be the first case of airline sabotage by a bomb with nitroglycerine as the probable explosive. A Chicago gangland murder was suspected. Passenger airliners as well as cargo aircraft have been the subject of plots or attacks ever since. For more details see Airline Attacks by Terrorists below.

1946: King David Hotel Bombing: Israel (91): Irgun, Jewish Terrorists

The King David Hotel bombing was carried out on the headquarters of the British authorities in then Palestine in Jerusalem killing 91 people and injuring 47. This terrorist attack was carried out by the Irgun, a militant Zionist group, intent on establishing a Jewish state. Menachem Begin a leading figure in Irgun at the time became a future Israeli Prime Minister and the Irgun is a predecessor of today's Israeli Likud party.

1948: Ben Yehuda Street bombing: Mandatory Palestine, Jerusalem by Palestinian Terrorists (58)

The Ben Yehuda Street bombings refer to a series of attacks by the Holy War Army forces, Palestinian irregulars, carried out on a major thoroughfare, named after the founder of modern Hebrew, Eliezer Ben Yehuda. Three stolen British Army trucks and an armoured car, exploded killing 58 Jewish civilians and injuring 140. A statement issued by the Arab High Command the following day claimed full responsibility and said the explosions were in retaliation for a Jewish Irgun bomb attack in Ramala.

1948: Mahatma Gandhi assassination by Hindu Nationalist Extremists

Indian political and spiritual leader Mohandas Karamchand (Mahatma' (Great Teacher)) Gandhi was murdered by a Hindu nationalist, Nathuram Godse, who fired three shots at close range as the 78-year-old Gandhi entered a prayer meeting. Gandhi had long been a leader of India's independence movement, preaching non-violent civil disobedience. He protested British rule and sought to improve the lives of Indians through frequent fasting and peaceful protesting. At the end of the second world war, Britain began to move toward granting independence, developing a plan for India to be partitioned into two countries, India and Pakistan, which would become independent in August 1947. The partition, which Gandhi opposed, caused the displacement of millions of Hindus and Muslims and widespread violence between the two communities. Gandhi continued to preach non-violence, which angered many Hindu nationalists who felt that Hindus needed to protect themselves from Muslim attacks. As Gopal Godse, brother and co-conspirator of assassin Nathuram Godse, explained before his death in 2005, Hindu extremists believed Gandhi's calls for non-violence were "part of a plot to allow Hindus to be slaughtered by Muslims." The Godse brothers and a team of conspirators carried out a failed bombing attack against Gandhi on 20 January 1948. Ten days later, their second assassination attempt succeeded. Nathuram Godse and Narayan Datatraya Apte were sentenced to death, while the other conspirators received prison sentences.

1963: US President John F Kennedy assassination by Lee Harvey Oswald

The 35th President of the US was assassinated while travelling through Dallas in an open-topped vehicle. Lee Harvey Oswald allegedly fired three shots from a rifle on the sixth floor of the Texas School Book Depository Building at 12.30pm. Kennedy was hit in the head and the throat, while one of Oswald's bullets also hit Texas Governor John Connally in the back. Oswald was himself later assassinated, provoking conspiracy theories that have endured to the present day.

1968: US Senator Robert F. Kennedy assassination by Sirhan Sirhan

Having just declared his victory in the California Democratic primary, moments later Robert Kennedy was attacked by Sirhan Sirhan as he was escorted through a kitchen pantry of the Ambassador Hotel. Kennedy was wounded by multiple shots from a pistol and died the following day. The attack, much like that suffered by his brother, has been surrounded by speculations of conspiracy. For instance a girl wearing a polka-dotted dress and a male companion were seen by multiple witnesses fleeing the scene shortly after the shooting. In April of 2012 CNN reported Nina Rhodes-Hughes's statement that Sirhan was not a lone gunman, but was accompanied by another shooter. Rhodes-Hughes, who stood feet away from Kennedy when he was murdered asserts

that "there was another shooter to my right".

1972: Israel's Lod airport attack by Japanese Red Army supported by the General Command of the Popular Front for the Liberation of Palestine (26)

Three Japanese Red Army (JRA) members arrived at Lod Airport (now Ben Gurion Airport) in Tel Aviv, Israel, via Air France Flight 132. They were dressed in business suits and carried what appeared to be violin cases. As the three men passed the ticket counter area, they opened their cases and took out automatic weapons and began to strafe the crowds. They also used hand grenades. One of the terrorists, Yasuyuki Yasuda, ran out of ammunition and was cut down by his companions. A second terrorist, Tsuyoshi Okudaira, committed suicide by pulling the pin on a grenade and detonating it against his body. The third terrorist, Kozo Okamoto, was captured while attempting to escape. In all 26 people were killed and 78 were injured. Whilst the target was Israelis or Jews, 16 of the dead were Puerto Ricans in Israel on a pilgrimage. Okamoto is the younger brother of Takeda Okamoto, one of the JRA terrorists who hijacked a Japan Airlines flight to North Korea in 1970. As the sole survivor of the Lod assassin team, Okamoto was sentenced to life imprisonment in Israel. He was released, however, as part of a 1983 prisoner exchange with Palestinian militant factions. He reportedly dropped from sight in Beirut, supposedly to reunite with his former comrades in the JRA. Investigations have shown that the JRA received considerable training and/or funds from Iran, Libya, Syria and the General Command of the Popular Front for the Liberation of Palestine. JRA was founded by Fusako Shigenobu, a Japanese woman who travelled to Lebanon in 1971 and founded the JRA, which then linked up with Palestinian extremists to become an enemy of Israel. She was best known for having masterminded the Lod Airport massacre. After the incident she made the following statement: "It is time to show the imperialists that armed struggle is the only humanistic way to advance the cause of oppressed people." In November 2000, Shigenobu was arrested in Osaka after being wanted by international law enforcement agencies for 26 years.

1972: Munich Olympics, Germany by Black September (19)

During the 1972 Summer Olympics in Munich in then West Germany, members of the Israeli Olympic team were taken hostage and eventually killed by the Palestinian terrorist group Black September. The Palestinian terrorists demanded the release of 234 prisoners held in Israeli jails. The terrorists eventually killed eleven Israeli athletes and coaches and a West German police officer. Five of the eight members of Black September were killed by police officers during a failed rescue attempt. The three surviving assassins were captured, but later released by West Germany following the hijacking by Black September of a Lufthansa airliner.

1973: Spanish Prime Minister Luis Carrero Blanco by ETA

Luis Carrero Blanco had only been prime minister by General Franco for about six months when he was assassinated. The 70-year-old, his bodyguard and a driver died instantly and four other people were injured after a remote-controlled bomb was detonated as he passed. The massive explosion sent the car hurtling into the air and over the roof of the San Francisco de Borga Church where Mr Blanco had just been attending mass. The vehicle landed on the second floor terrace of a building on the other side of the church causing also a great deal of damage to the area. Mr Blanco was opposed by many for propping up Franco's hardline regime, stifling opposition and for opposing mainstream European political life despite the country's progress in tourism and trade. Apparently the killers had dug a tunnel under the street the Prime Minister used regularly on his return from mass, with the killers triggering the bomb from an opposite basement in a well-planned assassination. Basque nationalists ETA, were blamed for the murder in retaliation for the execution of Basque militants in Spain, but the explosions also coincided with the start of a trial involving 10 of Spain's leading opponents of the Franco regime, one of them a Roman Catholic priest.

1974: The Birmingham pub bombings in UK by IRA (21)

The Birmingham pub bombings killed 21 people and injured 182, being placed in two central Birmingham pubs – the "Mulberry Bush" and the "Tavern in the Town" (now renamed the "Yard of Ale")². Although warnings were sent the pubs were not evacuated in time. The Provisional Irish Republican Army (IRA) was widely blamed for the bombings, although it denied responsibility. The bombings yielded a wave of anti-Irish sentiment and attacks on the Irish community in parts of Great Britain. A few days after, the Prevention of Terrorism Act was swiftly introduced by the British Government.

1978: Cinema Rex Arson in Abadan, Iran by Iranian Revolutionaries (477)

The Cinema Rex in Abadan, Iran was set ablaze, killing over 400 individuals by a group of Islamic extremists the moviegoers were violating Islamist beliefs by watching movies during the Islamic month of Ramadan. The single exit to the theater was locked with the assistance of a theater employee while the building was set ablaze with incendiary bombs. A small number of occupants were able to escape; most, however, were stampeded or died of smoke inhalation or flames.

1979: Hostage taking at Grand Mosque in Mecca, Saudi Arabia (includes 87 Islamic terrorists killed) (240)

200 Islamic terrorists seized the Grand Mosque in Mecca, Saudi Arabia, taking hundreds of pilgrims hostage. Saudi and French security forces retook the shrine after an intense battle in which some 250 people were killed

and 600 wounded. Hostage casualties included 26 killed and 109 injured; among Saudi soldiers, 127 were killed and 451 injured. At least 87 of the gunmen were killed and at least 40 injured; of those taken into custody, 67 were later simultaneously executed.

1979: Lord Mountbatten (Cousin of the Queen of England) in Ireland assassinated by IRA

Lord Mountbatten, a former decorated War Hero, last Viceroy of India, ex Chairman of NATO and a cousin of the Queen of England was assassinated by the Provisional Irish Republican Army (IRA), who planted a bomb in his yacht, the *Shadow V*, which had been left unguarded at Mullaghmore harbour, in the Republic of Ireland, just 12 miles from the border with Northern Ireland.³ One of the earl's twin grandsons, Nicholas, 14, and Paul Maxwell, 15, a local employed as a boat boy, also died in the explosion as did another passenger on the boat, the Dowager Lady Brabourne, 82, who died the day after the attack. Lord Mountbatten, aged 79, and his family had traditionally spent their summer holiday at their castle in County Sligo, north west of Ireland, but this was also an area of refuge for IRA operatives close to the border. The attack was followed only hours later by the massacre of 18 soldiers, killed in two booby-trap bomb explosions near Warrenpoint close to the border with the Irish Republic. A statement from the IRA said: "This operation is one of the discriminate ways we can bring to the attention of the English people the continuing occupation of our country." Thomas McMahon, was convicted of the three murders. McMahon was set free in 1998 under the Peace Accords, the Good Friday Agreement.

1978: Italian Prime Minister Aldo Moro kidnapped and assassinated by Red Brigade

In Italy in 1978, a former Prime Minister and Presidential prospect Aldo Moro was on his way with 5 bodyguards to see the then Italian Prime Minister when his car was ambushed by the Red Brigades, an Italian Terrorist group. All 5 bodyguards were shot and Moro taken. The terrorists demanded the release of 14 Red Brigades members imprisoned in Italian Jails. The Italian government refused to negotiate on principle and Moro was found murdered. Eventually in 1983, 32 terrorists were convicted on various charges connected with the Kidnap and Murder.

1979: US Embassy Hostage Crises, Tehran, Iran.

After President Carter agreed to admit the Shah of Iran into the US, Iranian radicals seized the US Embassy in Tehran and took 66 American diplomats hostage. Thirteen hostages were soon released, but the remaining 53 were held until their release after Carter left office in 1981.

1980: The Iranian Embassy Siege, London, UK.

A six-man terrorist team held the building for six days until the hostages were rescued by a raid by the SAS which was broadcast live on TV.

1981: President Anwar Sadat of Egypt assassinated by Al Gamaa al-Islamiyya

President Sadat was marking Egypt's Armed Forces Day, so called in commemoration of the Egyptian Third Army's launching of a surprise attack on that day in 1973 against Israeli forces occupying the Sinai since 1967, when several soldiers riding in a truck that was part of the military parade jumped to the ground, one throwing a grenade while others opened fire at Sadat and his entourage, killing Sadat. The attackers would eventually come to be identified as Islamist nationalists associated with the Muslim Brotherhood under the name of Egyptian Islamic Jihad.

The group was subsequently found to have hatched the assassination plot with Al Gamaa al-Islamiyya, a Brotherhood offshoot that would, in the mid-1990s, develop ties with Al-Qaeda and be chiefly responsible for the 1997 terrorist attack in Luxor on 17 November 1997, when six men dressed in black attacked tourists visiting the famous site in Upper Egypt. Sixty-two men, women and children were killed. Among the group's leaders: Ayman al-Zawahiri, subsequently Al-Qaeda's number 2. Zawahiri was tried and imprisoned for three years for his role in the plot, then expelled from Egypt. Al Gamaa al-Islamiyya accused Sadat of apostasy and condemned him for the peace treaty he'd signed with Israel.

1982: First truck bombing attack in Tyre Lebanon by Hezbollah (102)

On 11 November 1982, a Peugeot car packed with explosives struck the seven-story building used by the Israeli military to govern Tyre. The explosion leveled the building, killing 75 Israeli soldiers, border policemen, and Shin Bet agents. Between 14 and 27 Lebanese and Palestinians being held prisoner within the Israeli headquarters were also killed in the blast. The Israeli government asserted that the explosion was an accident, caused by the ignition of gas cylinders. This explanation stands in contradiction to the evidence of three witnesses who saw the Peugeot speed to the building, the identification of the car's parts in the rubble of the building, and the existence of a Shin Bet report detailing the Hezbollah preparations for the bombing.

1983: Truck bombings of US Marine and French barracks, Beirut, Lebanon by Hezbollah (301)

Terrorists attacked US and French troops stationed in Beirut as part of a UN peacekeeping Mission, exploding 2 truck bombs by crashing into Barracks at 6:30 a.m. Killing and injuring mostly sleeping soldiers. Within seconds, the four-story building collapsed taking with it the dead bodies of over 300 marines. The blasts led to the withdrawal of the international peacekeeping force from Lebanon, where they had been stationed since the Israeli 1982 invasion of Lebanon. Whilst the Islamic Jihad took responsibility for the bombing, it is thought to have been a nom de guerre for Hezbollah receiving help from Iran.

1983: Harrods Department Store bombing in London, UK by IRA (6)

On 17 December 1983, 6 fatalities and 90 injuries were caused by a car bomb planted in a side street near Harrods store in Knightsbridge, London. The attack was carried out by the IRA who sent a coded warning at 1245 GMT. Despite the damage Harrods reopened three days later.

1984: Margaret Thatcher, British Prime Minister attempted assassination by IRA (5)

The attack took place on 12th October 1984 at the Grand Hotel in Brighton, England. A bomb, constructed and planted by the IRA, detonated at 2.54am. Despite damaging her bathroom, Margaret Thatcher's bedroom and sitting room were unscathed, and the Prime Minister escaped without injury. Five people were however killed by the blast, including Conservative MP Anthony Berry and Parliamentary Treasury Secretary John Wakeham's wife Roberta. The following day the IRA claimed responsibility for the attack and vowed to make future attempts on the Prime Minister's life.

1984: Golden Temple Seizure, Amritsar, India by Sikh Terrorists (100)

Sikh Terrorists seized the Golden Temple in Amritsar, India. One hundred people died when Indian security forces retook the Sikh holy shrine.

1984: Indira Gandhi, Indian Prime Minister assassinated by Sikh Terrorists

Indira Gandhi was assassinated by Sikh Terrorists in the form of two of her Sikh bodyguards, Satwant Singh and Beant Singh. The two assailants opened fire as Indira Gandhi walked through the garden of the Prime Minister's Residence in New Delhi. 30 of the 31 bullets fired by Singh and Singh at close quarters found their mark. The attack came in the wake of Indira's attempt to crush a militant Sikh secessionist movement focussed in Amritsar. In so doing, Indira gave her approval to an assault on the Sikh Golden Temple shrine in which 100 people died, thus provoking outrage from the Sikh religious community.

1985: Attack on crowds in Sri Lanka by Tamil Tigers (150)

Tamil Tigers attacked crowds in Anuradhapura, Sri Lanka, with automatic weapons. Those attacked were mostly Buddhist worshippers and monks at Sri Maha Bodhi. The terrorists were dressed in army uniforms and drove through the area firing into crowds.

1985: Attack on Rome and Vienna airports simultaneously by Abu Nidal Organisation (15)

Twin terrorist attacks at Rome and Vienna airports were carried out killing 16 and injuring more than 100. Gunmen opened fire on passengers queuing to check-in luggage at departure desks for Israel's national airline, El Al. The attacks were indiscriminate and started within minutes of each other at about 8.15 in the morning.

The Palestinian terrorist group the Abu Nidal Organisation claimed responsibility.

1987: Bus attacks in Sri Lanka by Tamil Tigers (233)

Tamil Tigers first ambushed and attacked local Sinhalese travellers on three buses, two trucks, and a private van on a road in Sri Lanka near Alut Oya, killing 127 and injuring 64, continuing their attacks a few days after the road ambush, detonating a bomb at a bus depot in Columbo, Sri Lanka, killing 106 and injuring 295.

1990: Attack at mosques in Sri Lanka by Tamil Tigers (300)

Tamil Tigers attacked two mosques in Kathankudiy, Sri Lanka as Muslims filled the two mosques for daily prayer. The Tigers surrounded both mosques, one occupied by about 300, the other by about 40. The attackers fired through the windows and used other weapons. About 109 were killed immediately with another 31 later reportedly dying of injuries; another 70 were injured. The attacks were part of a series of attacks on Muslims in the area over a period of about a week, killing a total of about 300.

1991: Rajiv Gandhi Indian Prime Minister, by Tamil Tigers (15)

Indian Prime Minister, Rajiv Gandhi, was assassinated by Thenmozhi Rajaratnam on the 21 May 1991. Rajaratnam was a member of the Tamil Tigers and the Tamil National Retrieval Troops and wore an explosive belt concealed beneath her clothes. The assailant gained close access to Rajiv Gandhi amongst a crowd of well wishers greeting the former Prime Minister just before he was due to deliver a speech in Sripurumbudur. As she bent to touch his feet Rajaratnam detonated her explosive belt, killing Rajiv Gandhi and 14 others in the blast.

1992: Gold Mohur Hotel, Aden, Yemen by Al-Qaeda (2)

The first attack by Al-Qaeda was carried out in Aden, Yemen when AQ set off a bomb at the Gold Mohur hotel, where US troops had been staying while en-route to Somalia, though the troops had already left when the bomb exploded. The bombers targeted a second hotel, the Aden Movenpick, where they believed American troops might also be staying. That bomb detonated prematurely in the hotel car park, around the same time as the other bomb explosion, killing two Australian tourists.

1992: Israeli Embassy in Buenos Aires, bombed by Hezbollah (29)

A car bomb exploded at the Israeli embassy in Buenos Aires, killing 29 people and injuring more than 200. Whilst the Islamic Jihad claimed responsibility for the bombing, stating that it is in response to Israel's slaying of Shiite leader Sheik Abbas al-Musawi in February 1992. The US State Department believes the Islamic Jihad claim was a cover for Hezbollah. These Islamist terrorists are believed to have had support from the

tri-border region formed by the cities of Puerto Igauzu, Argentina; Foz do Iguazu Brazil; and Ciudad del Este, Paraguay which has a reputation for lawlessness and an historical presence of terrorist elements.

1993: Ranasinghe Premadasa, Sri Lankan President assassinated by Tamil Tigers (15)

Ranasinghe Premadasa was assassinated on 1 May 1993, during a May day rally, by a Tamil Tiger suicide bomber. Though no one officially claimed responsibility the Tamil Tigers of Tamil Eelam have been widely held responsible for the attack. At least 14 other people, including the police commissioner, were killed in the huge explosion in the centre of Colombo, police said.

1993: World Trade Centre bombing, US, New York City by Al-Qaeda (6)

The 1993 World Trade Centre bombing occurred when AQ operative Ramzi Yousef parked a rented van full of explosives in the parking garage beneath the World Trade Centre. The explosion claimed six victims, and over one thousand people were wounded. Ramzi Yousef, the nephew of 9/11 planner Khalid Sheikh Mohammed, had trained in Afghanistan, although Khalid Sheikh Mohammed did not join Al-Qaeda until 1998. Yousef worked in cooperation with the blind sheikh Omar Abdul Rahman in Jersey City, at the time of the attack. The FBI later turned up evidence that Osama bin Laden, who was never indicted for having a role in the bombing, provided financial support to the blind sheikh. Omar Abdul-Rahman.

1993: 15 bombings in Bombay, India by D- Company (317)

The bombings were a series of thirteen bomb explosions that took place in Bombay (now Mumbai), India on the same day in 1993. The coordinated attacks were the most destructive bomb explosions in Indian history. The single-day attacks resulted in over 300 fatalities and 700 injuries. The attacks are believed to have been coordinated by Dawood Ibrahim, head of the organised crime syndicate named D-Company, which had operated as a terrorist organisation. It is believed that the attacks were against Hindus and were carried out in retaliation for widespread massacres of Muslims in Mumbai during December and January, and also the demolition of the Babri Masjid. The targets included the Mumbai Stock Exchange building, banks, government offices, a hospital, an airline office (Air-India Building), and a major shopping complex. Most were car bombs but a scooter was also used and also a bus full of passengers was blown up. 3 hotels were also struck by suitcase bombs left in rooms booked by the terrorists.

1994: Asociacion Mutual Israelita Argentina (AMIA), bombed in Buenos Aires, Argentina by Hezbollah (86)

Terrorists bombed a Jewish community center killing 86. The investigations eventually implicated Hezbollah, the Lebanon-based Shiite Muslim militant organisation.

The primary suspect in the bombings is Imad Mughnayyah, a Hezbollah operative who is reportedly living in Iran. Argentine authorities believe that the attacks were organised in the tri-border region formed by the cities of Puerto Igauzu, Argentina; Foz do Iguazu Brazil; and Ciudad del Este, Paraguay which has a reputation for lawlessness and an historical presence of terrorist elements.

1995: Paris Metro bombing in Paris, France by GIA (8)

The attacks, which consisted of multiple bombings, were carried out by the Armed Islamic Group (GIA). This group attempted to extend the Algerian Civil War to France, claiming 8 lives in total and injuring more than 100 people. The first bombing took place on the 25th of July, when a gas bottle exploded in Saint-Michel station, killing 8 and wounding 80. 17th of August 17 people were wounded by a bomb detonated at the Arc de Triomphe. 26 August a bomb was discovered on high speed railtracks near Lyon, and on 3rd of September a bomb malfunctioned in a Paris square wounding 4. On 7th of September the GIA detonated a car bomb at a Jewish school in Lyon, injuring 14 people, and on 6th of October a gas bottle exploded at the Maison Blanche station of the Paris Metro. The final attack came on the 17th of October when a gas bottle exploded on train lines between Musée d'Orsay and Saint-Michel: Notre-Dame, injuring 29 people.

1995: Truck bombing of federal building, in Oklahoma City, USA by Anti Government Terrorist (168)

The attack carried out by Timothy McVeigh on the Alfred P. Murrah Federal Building in Oklahoma City was a domestic terrorist attack that claimed 168 lives and left over 800 people injured. Timothy McVeigh was arrested on a traffic violation and later charged with the bombing. McVeigh held anti-government views and chose the target a federal government building on the second anniversary of the federal raid on the Branch Davidian compound in Waco, Texas. Until the 9/11 attacks, it was the deadliest act of terrorism on US soil.

1995: Sarin subway station Attack, Tokyo by Aum Shinri-Kyu (12)

Tokyo Subway Station Attack, 20 March 1995: Twelve persons were killed and 5,700 were injured in a Sarin nerve gas attack on a crowded subway station in the centre of Tokyo, Japan. A similar attack occurred nearly simultaneously in the Yokohama subway system. The Aum Shinri-kyu cult was blamed for the attacks.

1996: Hostage taking in Budennovsk, Russia, by Chechen Terrorists (143)

75 Chechen Terrorists entered Budennovsk, Russia and attacked a police station, killing 42. The guerrillas then seized a hospital and took about 1,600 hostages. The terrorists killed initially 5 hostages (including 2 police officers). While about 400 hostages were released, Russian troops surrounded the hospital and made two un-

successful assaults over the next few days. These assaults freed about 200 hostages but resulted in many civilian casualties, most from a resulting fire in the hospital. A deal was eventually negotiated with the guerrillas under which they were permitted to return to Chechnya with about 200 hostages, mostly women and children, who were released at the Chechen border. Those killed include 18 policemen, 17 Russian servicemen, 94 Russian civilians, and about 14 terrorists;

1996: Khobar Towers bombing in Khobar Saudi Arabia by Al-Qaeda (19)

The Kobar Towers bombing was a terrorist attack on part of a housing complex in Saudi Arabia where foreign military personnel were stationed. The explosive device was concealed in a truck, killing 19 US servicemen and 1 Saudi on detonation. A further 372 individuals of diverse nationalities were injured in the explosion. Disagreements exist as to the identity of the culprits; however in 1996 the US rested responsibility for the attack with a group known as Hezbollah Al-Hijaz (Party of God in the Hijaz). Others have suggested that Al-Qaeda is the most likely orchestrator of the bombing.

1997/1998: Attacks at Ben Talha, and elsewhere in Algeria by Armed Islamic Group (1000+)

At the height of the Algerian Civil War, following the military cancellation of elections in 1997, that would have brought the Islamic Salvation Front to power, the Armed Islamic Group terrorized villages and towns mainly around the Capital, Algiers, massacring more than 1000 people over a period of months. One massacre, claimed the lives of 238 mostly pregnant women, babies, and the elderly. They were slaughtered, dismembered, and burned. In addition, more than 40 girls and women were kidnapped and later raped, then murdered, all of them residents of Sidi Rais near Sidi Moussa on the outskirts of the capital. Another massacre this time in the village of Hai-el-Djilali killed more than 200 villages, with the terrorists starting with explosions, then methodically going from house to house and killing men, women and children.

1998: US Embassy bombings in Kenya and Tanzania by Egyptian Islamic Group and AQ (303)

The embassy bombings were a series of attacks that occurred on August 7, 1998, in which 303 people were killed and an estimated 4,000 injured in simultaneous truck bomb explosions at the US embassies in the East African capitals of Dar es Salaam, Tanzania, and Nairobi, Kenya. The date of the bombings marked the eighth anniversary of the arrival of American forces in Saudi Arabia. The attacks were linked to local members of the Egyptian Islamic Jihad and Al-Qaeda. These attacks brought Osama bin Laden and Ayman al-Zawahiri to the attention of the American public for the first time, and resulted in the U.S. FBI placing bin Laden on its Ten Most Wanted Fugitives list. Although the attacks were directed at American facilities, the vast majority of casualties were local citizens; 12 Americans

were killed, including two Central Intelligence Agency employees in the Nairobi embassy, and one Marine at the Nairobi embassy.

The costs to the terrorists to carry out this attack have been estimated at US\$50,000. Earlier that year a Statement of intent had been signed and released by many Islamic Jihad Leaders from many Muslim countries, but most importantly by bin Laden which read "...In compliance with God's order, we issue the following fatwa to all Muslims: The ruling to kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can, in any country in which it is possible... We — with Allah's help — call on every Muslim who believes in God and wishes to be rewarded, to comply with Allah's order to kill the Americans and plunder their money wherever and whenever they find it. Unless you go forth, Allah will punish you with a grievous penalty, and put others in your place."

1998: Colombian Army ambushed by FARC (62)

FARC's military activity increased throughout the 1990s as the group continued to grow in wealth from both kidnapping and drug-related activities, while drug crops rapidly spread throughout the countryside. The FARC had thus managed to recruit and train more fighters, beginning to use them in concentrated attacks. This led to a series of high profile and successful attacks against Colombian state bases and patrols, but none more successful than in March 1988 when more than 700 FARC fighters ambushed the 52nd counter-guerilla battalion of the Colombian Army's 3rd Mobile Brigade, stationed at El Billar. The battalion had entered the town of Peñas Coloradas with the objective of damaging the FARC's infrastructure in the region. Nevertheless due to the FARC's influence and connections among the local population, the FARC were able to confront the battalion attacking it and causing heavy casualties and effectively eliminating it as an effective fighting force. Out of the 154 in the battalion 62 were killed and 43 were taken prisoner.

1999: Apartment bombings in Moscow Russia by Chechen Terrorists (301)

A bomb exploded in an apartment building in Moscow, Russia, killing 130 and injuring 150. Explosive had been placed in a rented room in the building. The explosion was one of four similar attacks on apartment bombings in a period of 12 days: the others killed an additional 62, 92 and 17 bringing a total of 301 fatalities for the four attacks. The Russian prime minister attributed the attack to Chechen Terrorists.

2000: Rizal Day bombings in Philippines on the Metro Manila by Jemaah Islamiyah(22)

The Rizal Day bombings were a series of attacks that took place in quick succession around Metro Manilla in the Philippines. 22 fatalities were recorded as a result of the bombings, and around a hundred suffered injuries. Despite almost three years of unyielding investigations,

by the close of 2003 responsibility for the attacks could be rested squarely with the Jemaah Islamiyah.

2000: USS Cole bombing, Yemen, Aden by Al-Qaeda in the Arabian Peninsula (19)

Al-Qaeda had planned to attack a US naval ship, the USS The Sullivans on January 3, 2000, by loading explosives on a small boat and then driving it into the Warship. This attempt failed due to too much weight being put on the small boat, but the setback with the USS The Sullivans, for Al-Qaeda turned to success shortly after when this technique was perfected in October 2000 with the USS Cole bombing, in Aden Yemen, killing 19. The costs to the terrorists to carry out this attack have been estimated at US\$10,000.

The attack was attributed to Al-Qaeda/Al-Qaeda in the Arabian Peninsula and foreshadowed the attack on the US less than one year later on September 11, 2001. Still whilst there was evidence, the US government had only formed a "preliminary judgment" that Al-Qaeda was responsible, with the caveat that no evidence had yet been found that bin Laden himself ordered the attack. Either because of these findings or as was stated by National Security Adviser later to the 9/11 Commission Condoleezza Rice, the decision not to respond militarily to the Cole bombing was President Bush's. She said he "made clear to us that he did not want to respond to Al-Qaeda one attack at a time. He told me he was 'tired of swatting flies.' The administration instead began work on a new strategy to eliminate Al-Qaeda, a strategy that would not have any material effect until the events of September 11, 2001.

2000/2004: Second Intifada Killings by Palestinian Terrorists in Israel (622)

The Second Intifada constituted the second Palestinian uprising and witnessed a prolonged period of intensified Palestinian-Israeli violence. This began in late September 2000 and ended around end of 2004, with multiple bombings occurring every year.

The year 2000 saw 5 bombings carried out by Hamas and the Palestinian Islamic Jihad, claiming 6 lives. 2001 witnessed 40 bomb attacks by Hamas, the Palestinian Islamic Jihad, and the Popular Front for the Liberation of Palestine. These attacks resulted in 85 deaths. 2002 saw 47 bombings perpetrated by Hamas, the Palestinian Islamic Jihad, the Popular Front for the Liberation of Palestine, Fatah and Al-Aqsa Martyrs' Brigades, which in total caused 246 deaths. 2003 experienced 23 bombings by these organisations, killing 124 people, and 2004 saw 18 bombings resulting in 98 deaths. The three most significant attacks in terms of lives lost came in 2002 with the Passover Massacre carried out by Hamas and Palestinian Islamic Jihad claiming 30 lives, 2003 with the Tel-Aviv central bus station massacre claiming 23 lives, and the Schmuel HaNavi bus bombing also claiming 23 lives in 2003.

Special Focus 1 2001: Attacks on America (9/11) by Al-Qaeda (2,997)



Four jetliners on domestic flights from north-eastern US airports were hijacked and crashed, three into buildings. Four or five hijackers aboard each aircraft used utility knives to subdue the crew, with a hijacker with flight training taking control of each aircraft. American Flight 11 was flown into

floors 94 to 99 of the World Trade Centre's north tower in New York City. United Flight 175 was flown into floors 78 to 84 of the Centre's south tower. Both crashes resulted in fires which eventually weakened the towers' structural steel, causing the complete collapse of the south and north towers. Most people not trapped by the fires had been evacuated from the towers at that point; however, hundreds of police officers and firefighters were in the towers. The World Trade Centre collapse caused fires and/or collapses of several nearby buildings, particularly World Trade Centre 7. AM American Flight 77 was flown into the Pentagon in Alexandria, Virginia, causing a fire and partial collapse of a limited section killing 125 Pentagon personnel, and injuring 200, and killing all 64 aboard the aircraft, including 5 terrorists. Passengers on the fourth jetliner, United Flight 93, learned of these events via cellular phones and attacked the hijackers; this aircraft crashed into a field in Somerset county, south central Pennsylvania, killing all 45 aboard (including 4 terrorists). The hijackers of this plane are believed to have intended to strike a site in Washington, DC, most likely the Capitol Building.

Fatalities due to the Trade Centre strikes remain uncertain at 2,759 dead; another 43 missing could not be conclusively linked to the World Trade Centre site. These figures include 343 firefighters, 60 police officers, 158 aboard the two aircraft, and 2,235 workers and visitors at the Trade Centre. Fatalities aboard the aircraft include 88 passengers and crew on American Flight 11, 60 passengers and crew on United Flight 175, and 5 terrorists on each plane. Total fatalities at the Trade Centre site include several hundred citizens of foreign countries: 27 were foreign residents (11 of the UK); 568 were born abroad. Foreigners included individuals from the UK, India, Columbia, Pakistan, Israel, and Puerto Rico. Another 8,700 were injured, of whom 6,391 received treatment. The attacks were conducted by Al-Qaeda with the operation overseen by Osama bin Laden and

the mastermind was Khalid Sheikh Mohammed. Total Fatalities believed to be 2,997.

It is believed that planning for these attacks had started as early as 1996 and that the focus of Al-Qaeda activity had been turned towards the US partly as a result of their support for Israel and partly as a result of AQ's fundamentalist religious beliefs. Those who would finally be involved in the plot as hijackers were subject to a rigorous selection process and only those who provided with details of the plot and financial support which is believed to have been made available by bin Laden. The hijackers then arrived in the US at different times during 1999 and 2000 and were split into two main groups, the first would receive technical flight training and the others would be used as physical support to help ensure entry was gained to the cockpit and that the passengers remained under their control.

Several of them then took flight training in California with one of their trainers subsequently noting that it seemed unusual that one of them had seemed somewhat disinterested in take-off and landing procedures but, as with many people who had contact with the hijackers during the planning phase, did not consider this to be worth reporting to the authorities. During this time, there was little that would have made the bank accounts used by the hijackers stand out from the huge numbers of other retail accounts and products being used by millions of others in the US.

Immediately after the attack the hijackers in an attempt both to identify others who may have been involved in the planning phase without perishing in the operation and also the source of the funding that would have been required.

US law enforcement quickly identified the hijackers and sent requests around the world to seek cooperation from other jurisdictions in an attempt to gather information as quickly as possible. Governments in these jurisdictions then sent requests to their financial institutions and banking records were quickly searched with many potential matches being forwarded to the US. That such action was coordinated so quickly was not just an indication of the extent and impact of the incident but also a demonstration of the financial community desire to do all it could to help to ensure that those responsible were quickly identified.

The 9/11 plot cost Al-Qaeda approx US\$400,000: US\$500,000 of which approx US\$300,000 was deposited into US Bank accounts for the benefit of the 19 hijackers. AQ funded the Hijackers in the US by three primary and unexceptional means i) wire transfers from overseas to the US, ii) the provision of physical

cash including directly from KSM as the hijackers transited Pakistan before coming to the US and cash deliveries and travellers cheques into the US and iii) the accessing of funds held in foreign financial institutions by debit or credit cards. Once in the US all the hijackers used the US banking system to store their funds and to facilitate their transactions. Whilst in the US the hijackers spent money primarily on flight training, travel, and living expenses (such as housing food cars and auto insurance). The hijackers returned approx 26,000 to a facilitator in the UAE in the days prior to the attacks.

The existing mechanisms to prevent abuse of the financial system did not fail. They were never designed to detect or disrupt transactions of the type that financed 9/11. The plot monies were provided solely by AQ. There was no evidence of and US domestic funding nor foreign government involvement or assistance. No evidence has come to light that any person with advance knowledge of the 9/11 attacks profited from them through securities transactions.

The 9/11 attacks brought Financial Institutions directly into the spotlight with governments expecting much more from financial Institutions to aid the fight against terrorism. Governments needed to cut off financing and follow money trails and so they needed financial institutions to step up and provide unprecedented support. Existing vulnerabilities in the international financial system which had been largely tolerated were targeted and as such the attacks also proved a turning point in the fight against money laundering.

The US quickly passed legislation implementing know your customer standards that only months before congress had roundly condemned. The International standard setters at FATF agreed 8 special recommendations to combat the war on terror (financing: CTF) and later added a 9th. Existing ML regulations were therefore strengthened and expectations dramatically rose. Failure to adapt and to adhere was not an option. FIs money laundering programmes were subjected to increased scrutiny and heretofore low regulatory risks and penalties migrated into increased regulatory penalties, civil and criminal sanctions and most importantly significant reputation damage in a worse case.

International wire transfers made up the majority of the funding for the 9/11 attacks the balance coming from cash couriered into the US and the use of foreign credit and debit cards. The following wire transfer activity took place between June and September 2000. On 29 June 2000, 20 year old Marwan al-Shehhi (designated

pilot and one of the leaders along with Mohammed Atta) received US\$5,000 at a Western Union facility in New York. The remittance was sent from the UAE in Dubai by a man who identified himself as Isam Mansar. Less than a month later, al-Shehhi received a second remittance from Mansar. On 18 July Mansar sent US\$10,000 via another bank transfer from Dubai to al-Shehhi's account at Sun Trust Bank. Three weeks later, on 29 August 2000, Ali Abdul Aziz Ali transferred US\$20,000 to the account owned jointly by Al-Shehhi and Mohammad Atta, using a phone number which differed from the phone number used by Mansar in previous transactions by only one digit. On 17 September 2000, Hani Fawaz Trading transferred US\$70,000 to the Sun Trust account, using the same Dubai exchange centre and the same telephone number as Aziz Ali. In less than one month US\$100,000 was transferred via the Dubai exchange centre to the same recipient from 3 separate transferors with almost identical telephone numbers. The Sun Trust Bank of Florida received, over a period of 3 months, a total of US\$109,400 in the Al -Shahhi/Atta account.

In retrospect, and with the considerable benefit of hindsight, there may have been transactions and activity that might have aroused concern but largely these assessments are based on the fact that a number of the hijackers may have had similar deposit and withdrawal pattern of activity but ignores the fact that similar patterns were almost certainly present in thousands of other retail accounts. Soon after the incident, much was made of the fact that a number of the hijackers had entered a banking hall together and, according to some reports, seemed unwilling to approach a female cashier but once again, even if true, it is something that is probably replicated many times each day and may also be behaviour that can only be identified as having been unusual and potentially suspicious in retrospect.

There are considerable amounts of information available about how the attacks were planned and carried out. Still this is really only of limited value. Whilst attempts have been made it has not been possible to establish a pattern in the financial activities of the hijackers that could be regarded as a useful typology for the future and also, from historical evidence, it seems that terrorist very rarely follow the same pattern as previous attacks – a logical reaction to the inevitable security enhancements that follow such an incident. Their ability to keep changing how they do things is aided both by the fact that there are many vulnerable targets and secondly that the sums of money required to commit such an attack are relatively small (certainly small when compared to the overall value of transactions flowing around the globe).

2001: Attack on a train in Angola by UNITA (152)
The Angolan Civil War had been raging since 1975 and was a legacy of the cold war, with the National Union for the Total Independence of Angola (UNITA) rebels still fighting the government. UNITA forces derailed a train travelling between towns of Zenza and Dondo about 150kms (93 mi) south-east of the capital, Luanda. After its derailment, rebels attacked the passengers with gunfire, killing around at least 152 of the 500 who were on the train.

2002: Bali Bombings in Indonesia by Jemaah Islamiyah (202)

A suicide bomber and a car bomb detonated outside popular nightclubs in Bali, Indonesia, with another bomb being detonated close to the US Consulate. The bombs killed 202 people including 88 Australian tourists. Three members of the violent Islamic group, Jemaah Islamiyah, were convicted and sentenced to death for the attack. The costs to the terrorists to carry out this attack have been estimated at US\$50,000.

2002: Theatre Hostage Crisis, Moscow, Russia by Chechen Terrorists (168)

Armed Chechen Terrorists Raided a Moscow theatre taking 850 hostages, demanding that Russia end the war in Chechnya. After using an unknown chemical, in an attempted rescue, Russian forces killed 39 rebels and 129 hostages.

2003: Red Square bombing in Moscow, Russia by Chechen Terrorists (6)

Carried out by the widow of a Chechen rebel commander this Chechen Terrorist suicide bombing killed 6 and injured 44. The bomber, identified as Khadishat Mangerieva, set off her explosive belt on a busy street. Reported speculation suggests that her intended target may have been the Moscow City Hall or State.

2003: Compound bombings in Riyadh, Saudi Arabia by AQ (35)

Late on 12th of May, several vehicles containing heavily armed men arrived at the three Riyadh compounds where a mixture of Americans, Westerners and non-Saudi Arabs were housed. A combination of shootings and bombings claimed the lives 35 people in total, while more than 160 were wounded. The attack was later claimed by Al-Qaeda.

2003: Bombings at British Bank and Consulate in Istanbul Turkey by AQ affiliate (57)

Four trucks loaded with bombs targeted synagogues, and the Turkish headquarters of HSBC Bank and also the British Consulate. The bombings killed 57 people and injured more than 700. A Turkish group affiliated with Al-Qaeda was prosecuted for planning and executing the attack with Osama bin Laden's approval. The costs to the terrorists to carry out this attack have been estimated at US\$40,000.

2003: Car bombing outside mosque in Najaf, Iraq by AQ Iraq (125)

This attack saw the detonation of two car bombs outside the Shia Imam Ali Mosque in Najaf on 29 August 2003. The explosion killed 83 people, including the religious leader Ayatollah Mohammed Baqir al-Hakim. The attack dealt a severe blow to the Shia community, as a result of both the large human cost in lives, as well as the loss of one of its most prominent leaders in al-Hakim.

According to US and Iraqi officials, Abu Musab al-Zarqawi was responsible for the attack. Al-Zarqawi headed the organisation al-Tawhid wal-Jihad, which later became known as Al-Qaeda in Iraq after al-Zarqawi pledged his allegiance to bin Laden in 2004.

2004: Two suicide bombings of political party offices in Irbil, Iraq by Kurdish Terrorists (109)

This attack comprised two suicide bombings, claiming the lives of 56 people and injuring at least 256 more. The bombs were detonated as hundreds gathered together to celebrate Eid Al-Adha in Irbil. No immediate claim of responsibility was made; however, radical Kurdish group known as Ansar Al-Islam operates in the Kurdish region and has been linked by US officials to Al-Qaeda.

2004: In N Uganda LRA rebels attacked a refugee camp (192)

In February 2004, the Lords Resistance Army attacked a refugee camp home to about 5,000 people killing 192 of them Armed with assault rifles, artillery and rocket-propelled grenades, rebels of the Lord's Resistance Army attacked Barlonyo camp in Uganda's Lira district. The camp was guarded by members of a local defence force, but they were outnumbered and outgunned. Led by Joseph Kony, who claims to have spiritual powers, the Lords Resistance Army have wreaked havoc across northern and north-eastern Uganda, forcing an estimated one million people to flee their homes. The group replenishes its ranks with children it abducts to use as fighters, porters or concubines.

2004: Superferry 14 bombing near Manila, Philippines by Abu Sayyaf (116)

A television set containing an 8-pound (4 kgs) TNT bomb had been placed on board. 90 minutes out of port, the bomb exploded. 63 people were killed immediately and 53 were missing and presumed dead. Despite claims from various terrorist groups, the blast was initially thought to have been an accident, caused by a gas explosion. However, after divers righted the ferry five months after it sank, they found evidence of a bomb blast. Abu Sayyaf admitted responsibility for the said incident killing 116. This act of terrorism was regarded as the world's deadliest terrorist attack at sea to date.

Special Focus 2

2004: Train Bombings in Madrid, Spain (3/11) by Al-Qaeda inspired (191)



In Madrid, Spain on 11 March 2004 ten explosions, packed into 13 rucksacks and detonated by cell phones, occurred on four commuter trains at the height of rush hour killing 191 civilians and injuring over 1,800. Police also carried out a controlled demolition of 3 other explosive devices.

The first group suspected of involvement was the Basque ETA, however investigations later focused on the Islamic extremist Moroccan Islamic Combatant Group (GICM), and links to Al-Qaeda. It was the deadliest attack on European civilians since the Lockerbie bombing of 1988 and in Spain it was the worst terrorist attack in its history.

The bombings targeted one of Spain's busiest arterial suburban commuter rail lines, which lies south east of downtown Madrid. These commuter lines carry an estimated 250,000 people out of the one million passengers the entire Spanish national rail network (RENFE) carries per day during the week.

The leaders of the group Fakhet and Ahmidan together planned and implemented the Madrid attacks, without any direct command and control from Al-Qaeda leadership. The group were largely common thieves and blue-collar workers, young, legal or illegal aliens mainly from Morocco (and to a lesser degree Algeria). Still this does not mean that the group operated in a vacuum or without reference to Al-Qaeda.

Even though the Madrid bombings were local in origin and had a local target, the bombers almost certainly saw themselves as part of the broader global jihad movement. Although there were no formal command and control links to Al-Qaeda, the network that carried out the bombings was plugged into the global jihad and took at least some of its impetus, inspiration, and legitimacy from that connection. Together The train bombings required neither external guidance, nor external resources. The finances for the Madrid bombings were self-generated. The 3/11 plot was followed on 2 April by an unsuccessful attempt to bomb the Madrid-Seville high-speed train. On 3 April 2004 as Spain's special forces closed in, having traced them through cell phone traffic, seven of the bombers including Fakhet blew

themselves up in an apartment in the Madrid suburb of Leganes. Had they survived it is suspected that they were likely to stage future suicide attacks in the months after the Madrid bombings.

The driving force behind the plot hatched in July 2003 and the carrying out of the bombings on 11 March 2004 was the relationship between Fakhet the Tunisian angry muslim radical and a Moroccan drug trafficker named Jamal Ahmidan. This relationship was decisive in turning Fakhet's anger into action and in allowing what had been a group of vocal radicals to develop the capacity to carry out a well orchestrated and highly lethal terrorist attack.

Serhane ben Abdelmajid Fakhet, a 35 year old who had come to Spain in 1994 to study economics at the University of Madrid had been a successful real estate salesman before undergoing some kind of personal crisis and subsequent radicalization. As part of this process – and probably both contributing to it and resulting from it: Fakhet developed close relationships with other extremists and became linked into those espousing global jihad. For example his brother in law had been arrested as part of a Spanish Al-Qaeda cell along with others after 9/11 and later bombings in Casablanca in 2003. Fakhet to an extent filled a vacuum left following arrests in Spain of Al-Qaeda suspects and his anger increased with Spain's strong support of the US and its involvement in Afghanistan and in particular the war in Iraq. Fakhet was deeply affected by the war in Iraq and started trying to persuade people to go there to wage jihad. He also sought Moroccan militants to assist with an attack in Spain, and having been rebuffed he was encouraged instead to recruit locally.

In this instance, it is believed that the offenders raised money by committing plastic card fraud and possible involvement in drug trafficking both of which generate or involve significant amounts of cash a fact which further removed the offenders need for or dependence on the banking system. The subsequent police investigation revealed that the terrorists had been planning the 3/11 attacks since August 2003. The terrorists had conducted surveillance on additional targets; had rented a safe house in Grenada (a city of tremendous symbolism for the jihadists), and had €1.5m cash-in-hand.

On the domestic counterterrorism front, Spain now realises it must confront the threat of Islamist militancy. A Spanish national defence directive puts terrorism as the number one threat to Spain's national security. The Spanish intelligence apparatus has re-oriented to focus increasingly on Islamic militancy, as well as the more traditional threat from ETA. The security services are placing agents in Muslim communities and the new socialist Government has instituted an outreach programme to improve links with Muslim communities in Spain.

The EU agreed to appoint a European security co-

ordinator and agreed in principle to a 'clearing house' arrangement for the exchange of information between Europol, Eurojust and EU member states' intelligence services. In 2003, Fakhet to an extent filled a vacuum left following arrests in Spain of Al-Qaeda suspects and his anger increased with Spain's strong support of the US and its involvement in Afghanistan and in particular the war in Iraq. Fakhet was deeply affected by the war in Iraq and started trying to persuade people to go there to wage jihad. He also sought Moroccan militants to assist with an attack in Spain, and having been rebuffed he was encouraged instead to recruit locally.

Ahmidan has often been described as the military planner for the Madrid bombings. This does not do justice to his role. He was the single most important individual in the execution of the Madrid attacks and without him the bombings would not have taken place. Ahmidan was the successful leader of a small, but effective drug trafficking group, which smuggled hashish from Morocco and ecstasy from Holland to Spain. He had a reputation for violence and a flashy life style. Although he, along with other members of his drug trafficking group, had grown up in Tetuan (a Moroccan town known for its extremists) as a young man, Ahmidan was not particularly religious. Even after migrating illegally to Spain, he was far more interested in his criminal business than political and religious extremism.

This changed, in part, as a result of his experience in prison in Spain and then in Morocco. One witness described Ahmidan as "very radical" and observed that it "was in the jail in Morocco, where he made contacts, where he was transformed. Now, he came to Spain to roll." He arrived back in July 2003, and by September he wanted to move his son from Catholic School to the Madrasah at Madrid's M-30 mosque. He also began to spend more and more time on the Internet looking at jihad sites.

Fakhet also had a profound impact on Ahmidan, crystallizing the process of radicalization already underway. Indeed, the relationship between Fakhet and Ahmidan is critical to the Madrid bombings.

The interactions between Fakhet and Ahmidan created an outcome that neither one would have achieved without the other. Fakhet brought to the relationship an infectious zealotry and a commitment to violence that would have probably come to nothing without Ahmidan's capacity to organise and implement. Without Ahmidan, Fakhet would probably have remained a "wannabe" terrorist, full of anger and resentment, but lacking the ability to turn his aspirations into

reality. And without Fakhet, Ahmidan would probably have continued to channel his drive, energy and organisational skills into his drug business rather than the "trains of death" project.

As it was, Ahmidan had assets which were indispensable in moving from concept to reality. The first was his charisma and leadership which brought along the other members of his drug trafficking organisation. A second was his contacts, some obtained from prison, which enabled him to obtain access to the dynamite that was used in the train bombings. The third was an ability to operate under the radar of law enforcement which led, for example, to the use of the safe house. Ahmidan also brought logistical expertise and provided "money, weapons, phones, cars, safe houses and other infrastructure".

Finally, and perhaps most important, Ahmidan acted as the financier of the attacks, using money, a stolen car, money from stolen cell-phone cards fraud and hashish to pay for the explosives, and covering the rentals for both the safe house and the apartment in Leganes as well as the cell phones used to detonate the bombs. In effect, the Madrid network was self-sufficient only because of Ahmidan and the use of proceeds from drug trafficking. The overall estimated cost came to US\$10,000, which did not include any outside funding.

The Madrid bombings have been directly accredited with changing the political landscape of Spain. The bombings occurred three days before the Spanish general elections on 14 March 2004. The PP, under the leadership of Prime Minister José María Aznar, was quick to lay the blame for the atrocity at the feet of the ETA.

It continued with this public line of reasoning even when evidence was emerging that Islamist radicals were the prime suspects. The public believed that the government had instituted a deliberate policy of misinformation for the purposes of political expediency.

A large proportion of the Spanish electorate deeply resented the war in Iraq and Spain's support for the US-led Coalition. In pointing the finger at ETA, it was commonly felt that the PP wanted to negate the charge that it had brought the attack on the Spanish people by following the US and UK into Iraq against the will of the majority of the Spanish electorate. This factor seems to have been the catalyst for the vote against the PP.

2004: Khobar massacre, Khobar, Saudi Arabia by AQ affiliate (22)

17 terrorists of the Jerusalem Squadron attacked the Arab Petroleum Investments Corporation building, the Petroleum Centre, and the Oasis Compound (a foreign workers' housing complex) in the city of Khobar, Saudi Arabia. After a 25-hour siege, 41 hostages were freed, 25 were injured and 22 were killed. Among the fatalities were 19 foreigners from nine countries. The nationalities of those killed included eight people from India, three from the Philippines, two from Sri Lanka, one each from Sweden, Italy, UK, US, South Africa and Egypt. 14 of the terrorists were captured or killed, while 3 escaped. The attack is thought to have been religiously motivated, with the kidnappers asking their hostages whether they were Christian or Muslim. Muslim prisoners were consequently freed, while non-Muslims were detained. A previously unheard-of militant group calling itself "The Jerusalem Squadron", a local Saudi Arabia-based faction of Al-Qaeda, claimed responsibility and said it was attacking "Zionists and Crusaders" who are guilty of stealing oil from Saudi Arabia.

2004: Multiple suicide bombings at shrines in Kadhimiya and Karbala, Iraq by Sunni insurgents / AQ in Iraq (188)

The Ashura massacre of 2 March 2004 in Iraq was a series of planned terrorist explosions killing 188 and injuring at least 500 Iraqi Shi'a Muslims who were gathering to commemorate the Day of Ashura. The bombings brought one of the deadliest days in the Iraq occupation after the Iraq War to topple Saddam Hussein and was thought to be carried out by Al-Qaeda in Iraq.

2004: Multiple bombings and armed attacks in several cities in Iraq by Sunni Insurgents / AQ in Iraq (103)

23 May 2005, 3 fatalities and more than 70 injuries followed the detonation of a car bomb outside a restaurant in northern Baghdad around midday. Several other suicide bombings and attacks left at least 10 people dead across the country. One attack saw the Iraqi general Wael al-Rubaie killed by gunmen in the Mansour district of Baghdad. In Baghdad's southern Dora neighbourhood unknown gunmen killed a policeman as he was heading to work at a local court, police said. An attack in the town of Tuz Khormato, about 125 miles north of Baghdad, also caused 5 fatalities and 13 serious injuries when a suicide bomber blew up a truck after driving it into a crowd that was waiting for a council office to open. A further incident in Samara left two Iraqis dead when 3 suicide bombers launched an attack against a US military base. Insurgents escalated attacks following the announcement in late April of a new government, killing more than 500 people in suicide bombings, assassinations and ambushes. The attacks were thought to be carried out by Sunni Insurgents and Al-Qaeda in Iraq.

2004: School Hostage Crisis, Beslan Russia by Chechen Terrorists (334)

Chechen Terrorists stormed the Comintern Street SNO school in Beslan, North Ossetia, Russia on the first day of a new term on 1 September 2004, all heavily armed wearing green camouflage and black balaclava masks with some wearing explosive belts. The attackers took the 1,100 hostages into the school gymnasium. The attackers killed the male teachers and fathers of pupils instantly as they were identified as potential threats with many hostages remaining being the Children. The hostage siege lasted 3 days when Russian security forces stormed the school, leading in all to 334 killed, including 186 children and 783 injured.

2004: Akhmad Kadyrov (President of Chechnya) assassinated by Chechen Terrorists

9 May 2004, Akhmad Abdulkhamidovich Kadyrov fell victim to a bomb blast that hit the VIP section of the Dinamo football stadium during a World War II memorial victory parade. The bomb was planted by Chechen Terrorists continuing their insurgency campaign

2005: Rafik Hariri (Lebanese Prime Minister) assassinated by Hezbollah

In February, 2005, former Prime Minister of Lebanon was killed by an explosion equivalent to around 1,000 kg of TNT (2,200 pounds) hit his motorcade near to the St George Hotel in Beirut. The attack is widely believed to have been undertaken by Hezbollah and claimed 21 other lives besides that of Hariri.

2005: Amman bombing in Amman, Jordan by AQ affiliate (60)

The Amman bombings were a series of coordinated bomb attacks centred on three hotels in the city: The Grand Hyatt Hotel, The Radisson SAS Hotel, and the Days Inn. In total the attacks caused 60 fatalities and 115 injuries. The hotels were selected due to the high number of foreign diplomats, military contractors, journalists and business people that frequented them. The attacks were carried out by Al-Qaeda affiliated terrorists.

2005: New Dehli Bombings, India by Pakistan Kashmiri Separatists (62)

During the Hindu festival of Duvali, three bombs went off in New Dehli, India, killing 62 and wounding 210. The bombs were placed in a car, a motorcycle and on a bus. Indian officials believe the bombs came from Pakistan Kashmiri separatists.

2005: Car bombing outside medical clinic in Hilla, Iraq by AQ in Iraq (125)

In February, 2005, a car bomb detonated outside the Popular Clinic in Hilla claimed the lives of 125 people. The majority of those queuing outside the clinic were waiting for medical tests required to work in Iraq's health and education ministries, and its security forces. Al-Qaeda in Iraq claimed responsibility.

Special Focus 3

2005: London Trains & Bus Bombings, UK (7/7) by Al-Qaeda Inspired (52)



On 2 June 2005 the UK Intelligence authorities lowered the UK national alert state from "severe general" to "substantial" with the words "at present there is not a group with both the current intent and the capability to attack the UK"

Nevertheless, on Thursday 7 July four explosions took place in London within a very short space of time. Three had occurred on London Underground trains whilst the rush hour was just ending and the fourth tore the top of a double decker bus a few minutes later. The City of London ground to a halt as emergency services rushed to the scene. 56 people, including the four bombers, died with over 700 injured. The attacks, motivated by Al-Qaeda, were nevertheless carried out by four young British born men 3 with Pakistani and 1 with Jamaican and all with Islamic heritage none of whom had previously been involved in significant criminal activity or were actively known to intelligence agencies as likely terrorists.

The leader Mohammad Sidique Khan had been on the fringes of activity being monitored by the UK security services, but he had not been tracked or under surveillance at the time of and before the attacks. The men had been radicalised in the years after 9-11 claiming western involvement in Afghanistan and Iraq provided a basis for their actions. Each of the four terrorists had made trips to Pakistan – and it is believed also into Afghanistan. In the weeks leading up to the attack they had been constructing the bombs in a flat and people close to them had noted that they wondered whether they had been dying their hair as it had started to change colour. In reality, this was the effect of the chemicals being used to construct the explosive devices.

On the morning of 7 July they used a rental car to drive to Luton station and then boarded a train before separating and getting on different underground trains where three were subsequently successful in blowing

themselves up together with other passengers on the train. It is believed that the fourth member failed to detonate his bomb and so exited the tube where he is thought to have purchased a battery and tried to phone his associates but having got no response was able to tell that they had carried out their intentions. He then boarded a bus and exploded his bomb ripping off the top deck. Police almost immediately identified three of the offenders and a search of the flat revealed so much incriminating evidence that it was clear that the four had no intention of returning. According to then Chancellor Gordon Brown "enquiries following the attacks of 7 July have demonstrated the crucial role of terrorist finance investigation and high quality reporting by financial institutions pointed to strong private sector engagement with the UK counter terrorism effort."

Immediately after the explosions a massive police and intelligence effort was launched to identify those responsible and to prevent further attacks. In the first hours after the bombings a financial investigation exercise commenced and after contact had been made with financial institutions, personal items, cash and memberships cards, a credit card and a driving license were found in the names of those suspected as the bombers at the incident sites. From this information the names of the possible bombers were provided to Financial Institutions who then searched their client databases and provided authorities quickly with information to allow the investigators to establish a comprehensive financial footprint for each of the bombers. Every line in bank statements were analysed, links were quickly identified.

The leader of the group MSK had a reasonable credit rating, multiple bank accounts (each with a small sum deposited for protracted periods), multiple credit cards, including from HSBC (with £4,000 being withdrawn in Cash). MSK had taken a loan of £10,000 from Barclays Bank but had recently defaulted on repayments and was overdrawn on his accounts. He did though have two periods of intense activity in October 2004 and before the attacks. The cost of the bombings were largely self financed by MSK. The total cost for the bombings amounted to under £10,000. This was made up of £4,600 for construction and deployment of devices, with the actual bomb making materials amounting to £2,500, international travel £1,800 and weekends away for training £825. This operation required very little finance, was self funded from legitimate means, and was not capable of identification by financial institutions prior to the bombings. The loan was raised in the normal course and the hire car was arranged using a credit card for which the bill had not been issued prior to the explosions. Nevertheless the contribution

from the financial sector, the speed of response and the importance and accuracy of the information provided was a critical component in the post bombing investigation and led to further investigations and prosecutions beyond those directly involved. For example a financial institution provided information about an expenditure charged to a credit card in an outdoor clothing store which included a rucksack – and the investigators rang the store to establish whether or not CCTV footage existed. The store member didn't recall that transactions but did remember that he had sold almost the same items to another person and was able to trace the receipt through which process the police finally identified the fourth and final bomber.

The fact that the levels of finance were so low coupled with the fact that the offenders lifestyle did not change until very close to the event meant that no significant profiles in their financial accounts was likely to be detected. It has been debated whether in the case of domestic Islamic terrorism, a financial profile could be compiled which includes personal details similar to those of the bombers (for example age, islamic connections, foreign long stay travel to pakistan and or afghanistan.) A financial Institution may identify such long stay travel by use of credit or debit cards, for example regular use in the UK may be superseded by sporadic use in Pakistan over an extended period.

2005: Sharm el-Sheikh Resort Attacks, Egypt by Al-Qaeda affiliate (88)

Abdullah Azzam Brigades, an Al-Qaeda affiliate, attacked the Egyptian resort town of Sharm el-Sheikh setting off a series of explosions that killed 88 and injured over 200. A car bomb, a suitcase bomb and a truck bomb all detonated in the downtown area of Sharm el-Sheikh as well as a popular tourist hotel. Abdullah Azzam Brigades, a group tied to Al-Qaeda, took credit for the attack and cited the war in Iraq as their motivation.

2005: Multiple suicide bombings and shooting attacks in Baghdad, Iraq by AQ in Iraq (182)

On 15 September, Iraqi insurgents killed 182 and injured more than 500 by exploding at least 12 co-ordinate suicide attacks. The attacks appeared to be retaliation for the siege by government forces of the insurgent stronghold of Tal Afar and included a bombing in a Shi'ite neighborhood of Baghdad that used a new tactic: luring scores of day labourers to a minivan with promises of work, and then blowing it up. At least 112 died in that blast alone, the second highest death toll from any single terrorist bombing in Iraq since the invasion. The attacks coincided with the opening of the UN General Assembly in New York, attended by top Iraqi leaders and President Bush, who pressed for a resolution calling on all nations to take action against the incitement of terrorism. The explosions struck Shi'ite civilians,

Iraqi security forces and American troops, the favored targets of Iraq's Sunni Arab insurgency. The worst attack singled out workers in a Shi'ite neighborhood, Kadhimiyah, with an explosion that tore through a crowded intersection, leaving the facades of nearby shops shattered and puddles of blood on the streets. Hours after the first attack, Al-Qaeda in Iraq issued a statement claiming responsibility.

2006: Central Mindanao bombings in Philippines by the Moro Islamic Liberation Front (MILF) (8)

The Central Mindanao bombings constitute a series of three bombings and one failed bombing in Central Mindanao on October 10 and 11. Eight people were killed and 30-46 were injured. The Moro Islamic Liberation Front (MILF) were blamed whilst others suggest the Abu Sayyaf or Jemaah Islamiyah (JI) was behind the attacks, as the arrest of Istiada Binti Oemar Sovie, the wife of JI leader Dulmatin, in Sulu may have prompted the attacks. Dulmatin himself is reportedly hiding on Jolo Island.

2006: Bombings in Karbala, Ramadi, and Baghdad, Iraq by sectarian militants by AQ in Iraq (124)

Al-Qaeda in Iraq suicide bombers targeted Karbala shrine and a police recruiting station in Ramadi, killing 110 people. The attacks were intended to destabilize the political process, which was at the time working towards the formation of a common coalition government between Shia, Sunni and Kurdish parties.

2006: Multiple bombings on commuter trains in Mumbai, India By Lashkar-e-Tayyiba & Students Islamic Movement of India (SIMI)(200)

A series of seven bomb blasts took place over a period of 11 minutes on the Suburban Railway in Mumbai, the capital of the Indian state of Maharashtra and the nation's financial capital. The bombs were set off in pressure cookers on trains plying the Western line of the Suburban Railway network. Each pressure cooker contained a 2.5 kg mixture of RDX and ammonium nitrate. 209 people were killed and over 700 were injured. Mumbai Police reported that the bombings were carried out by Lashkar-e-Tayyiba and Students Islamic Movement of India (SIMI).

2006: Truck bombing of military convoy near Habarana, Sri Lanka by Tamil Tigers (103)

Also known as the Habarana massacre, the attack was a suicide truck bombing executed by the Tamil Tigers. The attack targeted a convoy of 15 military buses carrying more than 200 sailors from Trincomalee. The bombing resulted in 92-103 fatalities and wounded more than 150 people. Also caught up in the attack were a number of civilians, some of whom lost their lives.

2006: Sadr City bombings in Baghdad, Iraq, by Sunni Insurgents/AQ in Iraq (215)

In November, Suni Insurgents Al-Qaeda in Iraq placed

6 car bombs and used two mortar rounds in the attack on the Shia slum in Sadr City, killing at least 215 and injuring more than 250 people, making it at that time the second deadliest sectarian attack since the beginning of the Iraq Civil War in 2003.

2007: Multiple bombings in Baghdad area, Iraq by Sunni Insurgents/AQ in Iraq (101)

18 April, 2007: Around 140 people were killed in a car bombing in a food market in Sadr City district. The suicide attack, by Sunni Insurgents/AQ in Iraq taking place at 1600 (1200 GMT), killed at least 135 people and injured 339 others. About an hour before the attack on the market place in the Sadr City district a suicide car bomb attack on a police checkpoint in Sadr City also killed 35 people. A car bomb near a private hospital in the Karrada district claimed the lives of 11 more victims, and a minibus bomb in the Al-Shurja took a further 11 lives.

2007: Truck bombing in market place in Baghdad, Iraq by Sunni Insurgents/AQ in Iraq (137)

3 February, 2007: The detonation of a large truck bomb in a busy market in the Iraqi capital of Baghdad killed 137 people and injured 339 others. The bomb, estimated to be about one ton in weight, brought down at least 10 buildings and coffee shops and obliterated market stalls in a largely Shi'ite enclave less than a half mile from the Tigris River. The bombing was carried out by Sunni Insurgents/AQ in Iraq.

2007: Two bombings and other attacks on pilgrims, Hillah, Iraq by Sunni Insurgents/AQ in Iraq (115)

The 2007 Al Hillah bombings killed 115 people, mostly Shia Muslims on a pilgrimage, on 6 March 2007 in Al Hillah, Iraq. The bombing was carried out by Sunni Insurgents/AQ in Iraq.

2007: Two truck bombings in Tal Afar, Iraq by Sunni Insurgents/AQ in Iraq (152)

The 2007 Tal Afar bombings took place on March 27, 2007, when two truck bombs targeted Shia areas of the town of Tal Afar, Iraq, killing 152 and wounding 347 people. The bombing was carried out by Sunni Insurgents/AQ in Iraq.

2007: Bombings in Baghdad, Iraq by Sunni Insurgents/AQ in Iraq (193)

The 18 April 2007 Baghdad bombings were a series of attacks that occurred when five car bombs exploded across the capital, on 18 April 2007. The explosions killed nearly 200 people and targeted mainly Shia locations and civilians. The Sadr City market had already been struck by a large truck bombing on 3 February 2007 and was in the process of being rebuilt when the attack took place. The bombings were reminiscent of the level of violence before Operation Law and Order was implemented to secure the Iraqi capital in February 2007. The attacks came as Iraqi Prime Minister Nouri al-Maliki asserted that Iraqi forces would assume control of the

country's security by the end of the year. The attacks also coincided with the arrival of officials from more than 60 countries in Geneva to attend a UN conference on the plight of Iraqi refugees. The bombing was carried out by Sunni Insurgents/AQ in Iraq.

2007: Hostage taking by Sunni radicals and subsequent storming of mosque in Islamabad, Pakistan (102)

Sunni radicals and followers of the radical cleric Maulana Abdul Aziz held four policemen hostage in Islamabad's Red Mosque. The kidnappers sought the imposition of Sharia law and openly called for the overthrow of the Pakistani government. The complex was besieged from 3 July to 11 July 2007, while negotiations were attempted between the militants and the State. Once negotiations failed, the complex was stormed and captured. The conflict resulted in 154 deaths, and 50 militants were captured. A further consequence of the assault was the nullification of a 10-month-old peace agreement between the Pakistan Government and pro-Taliban rebels along the Afghanistan border. This event triggered the Third Waziristan War, which marked another surge in militancy and violence in Pakistan and has resulted in more than 3,000 casualties.

2007: Multiple truck bombings in Al-Qataniyah and Al-Adnaniyah, Iraq by Sunni Insurgents / AQ in Iraq (796)

The worst of all the attacks in Iraq caused a death toll close to 796 people injuring 1,562. Four coordinated suicide truck bomb attacks detonated in the Iraqi towns of Qahtaniya and Jazeera (Siba Sheikh Khidir), near Mosul. The bombings were targeted at Yazidi, a Kurdish religious minority in Iraq and were carried out by Sunni Insurgents/AQ in Iraq.

2007: Truck bombing in Armili, Iraq by Sunni Insurgents / AQ in Iraq (105)

A truck carrying 2 tons of explosives detonated in a northern Iraqi busy outdoor market in the village of Armili which is populated largely by Shi'ite Turkmen and Kurds, killing at least 105 and wounding another 250. The truck was disguised as a military vehicle. This attack followed a string of recent bombings that killed almost 50 Iraqis and 10 American soldiers in the previous days. The bombings were carried out by Sunni Insurgents/AQ in Iraq.

2007: Bombing of motorcade in Karachi, Pakistan in an attempted assassination of Benazir Bhutto by Pakistan Taliban (137)

The assassination attempt failed when a bomb exploded targeting the motorcade of the former Prime Minister Benazir Bhutto, killing many including 50 of her security guards but leaving Bhutto uninjured. As the convoy slowly approached a bridge in Karachi, a militant Islamic terrorist from the Pakistan Taliban first threw a grenade near the convoy, then he approached Bhutto's vehicle detonating explosives. This larger

explosion occurred a few meters from Bhutto's vehicle, setting a police escort van on fire, and breaking windows in Bhutto's truck. Two police vehicles were destroyed. The bombing occurred two months before she was assassinated. The bombing resulted in at least 139 deaths and 450 injuries. Most of the dead were members of the Pakistan Peoples Party.

2007: Assassination of Benazir Bhutto in Pakistan and others by Pakistan Taliban (24)

Benazir Bhutto, former Pakistani prime minister, was killed in a bombing at a campaign rally in Rawalpindi, Pakistan by a suicide bomber and a Pakistan Taliban leader with close ties to Al-Qaeda cited as the assassin.

2007: Algiers, Algeria bombings by AQ affiliate (33)

Al-Qaeda Organisation in the Islamic Maghreb claimed to have been responsible for bombings within a short time of each other, one at the prime ministers office and the other at a police station. The blasts killed 33 people. It was the first time a bombing had occurred in the capital in more than a decade.

2007: Algiers, Algeria bombings by AQ affiliate (60)

As many as 60 people were killed in two suicide attacks near UN offices and government buildings in Algiers, Algeria. The bombings occurred within minutes of each other. Al-Qaeda in the Islamic Maghreb, formerly called the Salafist Group for Preaching, claimed responsibility.

2008: Bombing at dog fighting festival in Kandahar, Afghanistan by the Taliban (105)

In 2008, at least 65 people lost their lives when a bomb exploded at a dog fighting festival in Kandahar. The primary target of the attack was reported to be Abdul Hakim Jan, an anti-Taliban militia leader and former police chief prior to the Taliban assumption of power. Abdul Hakim Jan died in the blast carried out by the Taliban.

2008: Mumbai Attacks, India by Lashkar-e-Tayyiba 26/11 (164)

The 2008 Mumbai attacks were twelve coordinated shooting and bombing attacks across Mumbai, India's largest city by members of Lashkar-e-Tayyiba, the Pakistan-based terrorist organisation. The attackers allegedly received reconnaissance assistance before the attacks. Ajmal Kasab, the only attacker who was captured alive, later confessed upon interrogation that the attacks were conducted with the support of Pakistan's Intelligence service (ISI). The attacks, began on Wednesday, 26 November and lasted until Saturday, 29 November 2008, killing 164 people and wounding at least 308. Eight of the attacks occurred in South Mumbai: at Chhatrapati Shivaji Terminus, the Oberoi Trident, the Taj Mahal Palace & Tower, Leopold Cafe, Cama Hospital (a women and children's hospital), the Nariman House Jewish community centre, the Metro Cinema, and a lane behind the Times of India building and St Xavier's College. There was also an explosion in

Mumbai's port area, and in a taxi. By the early morning of 28 November, all sites except for the Taj hotel had been secured by Mumbai Police and security forces. On 29 November, India's National Security Guards (NSG) conducted Operation Black Tornado to flush out the remaining attackers; it resulted in the deaths of the last remaining attackers at the Taj hotel and ending all fighting in the attacks.

2008: American Embassy attack in Sana'a Yemen by Islamic Jihad of Yemen (AQ affiliate) (19)

An attack on the American Embassy in Yemen resulted in 19 deaths and 16 injuries. The attack was the second in 2008, with a mortar attack in March narrowly missing the embassy and hitting a nearby girls' school. The Islamic Jihad of Yemen, an Al-Qaeda affiliate, claimed responsibility for the attacks. The group also threatened future attacks against other foreign embassies, including those of Saudi Arabia, the United Arab Emirates and the UK.

2008: Christmas Attacks in North DRC and South Sudan by Lords Resistance Army (865)

In late 2008 and early 2009 including attacks on Christmas day itself, the Lords Resistance Army (LRA) brutally killed more than 865 civilians and abducted at least 160 children in mostly Northern DRC, but also South Sudan. The LRA hacked their victims to death with Machetes or axes and crushed their skulls with clubs and heavy sticks. Over a 48 hour period around Christmas day in 3 locations only 160 miles apart, the LRA used the time to attack knowing that more families would be together and so make their attacks all the more devastating. Before shifting it focus to the DRC in 2006 the LRA was largely based in Uganda. The LRA attacked the villagers because some had helped LRA defectors escape.

2009: Uprising In Borno State Nigeria by Boko Haram (780)

In July 2009, police arrested several leaders of Boko Haram on suspicion they were preparing for violence, with intelligence indicating the group was planning to over-run Bauchi city, in Borno state. Protesting the arrests, and probably also trying to free their detained leaders, several hundred members attacked the police station in Bauchi but they were repelled and at least 50 of them killed. For the next four days, the group battled police, reinforced by the army, in Bauchi, Borno, Kano and Yobe states. The worst violence was in Maiduguri, where the group was based. It is estimated by the Red Cross that at least 780 people were killed buried in mass graves. The Police listed 28 of its officers as among those killed.

2009: Multiple bombings at government sites in Baghdad, by Sunni Insurgents and AQ in Iraq (102)

The 19 August 2009 Baghdad bombings were three coordinated car bomb attacks and a number of mortar strikes in the Iraqi capital, Baghdad. The explosives went

off simultaneously across the capital at approximately 10:45 in the morning, killing at least 101 and wounding at least 565. It was therefore the deadliest attack since the 14 August 2007 Yazidi bombings in northern Iraq which killed almost 800 people. The bombings were targeted at both government and privately-owned buildings. Organisational responsibility for the attacks was not established definitively, though the plots mastermind, Munaf Abdul Rahim al-Rawi, was arrested in 2010. Al-Rawi was integrated into the Al-Qaeda in Iraq network, however suggestions of involvement were also leveled at both Syria and Iran.

2009: Two car bombs explode at government buildings in Baghdad, Iraq carried out by Sunni Insurgents and AQ in Iraq (155)

In October a pair of suicide car bombings devastated the heart of Iraq's capital, killing 155 people in the country's deadliest attack in more than two years. The bombs targeted two government buildings killing 35 employees at the Ministry of Justice and at least 25 staff members of the Baghdad Provincial Council, with at least 721 people were wounded. The bombings were carried out by Sunni Insurgents/AQ in Iraq.

2009: Bombing at marketplace in Pakistan by Pakistan Taliban militants (118)

11th November 2009: The blast from the car bomb delivered by a Taliban suicide bomber occurred in Charsadda, about 25 miles northeast of Peshawar. 34 people were killed in the third terrorist attack striking the area in three days. The attacks were provoked by the conflict between Pakistan armed forces and Taliban militants in the South Waziristan tribal region along the Afghan border.

2009: Five car bombings in Baghdad, Iraq by Sunni Insurgents/AQ in Iraq (127)

The attack occurred on the morning of 8 December 2009, at approximately 10:30 am. Local residents reported one blast just after 10:00, followed about half an hour later by another four blasts in quick succession. By mid-afternoon, officials had reported five blasts in the area. At least four of the attacks are believed to have been coordinated. The first of the bombings targeted a police patrol in Dora; this attack also wounded several people at a nearby college. The next four bombings were believed to be targeted at government buildings, and were detonated by suicide bombers. Islamic State of Iraq has claimed responsibility for these four attacks; however it remains unclear whether the attack in Dora was of their making. Burnt out vehicles, believed to be the ones used for the bombings, were found outside the Finance, Foreign, and Justice Ministries. At least 121 people were killed in the combined attacks. The attacks were carried out by Sunni Insurgents/AQ in Iraq.

2010: Multiple bombings in Hilla, Basra, al-Suwayra, and other cities, Iraq by Sunni Insurgents and AQ in Iraq (102)

Shootings and suicide bombings occurred in several Iraqi cities on the 10th of May 2010, resulting in more than 100 fatalities and 350 injuries. The central city of Hilla saw the deadliest attack, when staff at a textiles factory were hit by three bomb attacks, killing at least 45 people. The violence began with a series of drive-by shootings targeting police and army officers in the capital Baghdad, carried out by Sunni Insurgents and AQ in Iraq.

2010: Metro bombings in Moscow Russia by Chechen Terrorists (40)

The 2010 Moscow Metro bombings were suicide bombings carried out by two women during the morning rush hour on the Moscow Metro system. The two stations targeted on 29 March 2010 were Lubyanka and Park Kultury, with roughly 40 minutes interval between the blasts. At least 40 people were killed, and over 100 injured. In the days following the attacks it emerged that the perpetrators were Chechen Terrorists.

2010: Attack in Dantewada India by Maoist Terrorists (76)

The explosion on 17 May 2010 was triggered when a bus hit a landmine 50km away from Dantewada, in Chhattisgarh's Dantewada district. Fatalities reports range from 31 to 44, including several Special Police Officers (SPOs) and civilians. It was the first attack by Maoist Terrorists (also known as Naxalite-Maoist insurgents) to target a civilian bus.

2010: Bombings in Zahedan, Iran by Jundullah (27)

A twin suicide bombing in Zahedan collectively killed 27 and wounded approximately 300. These attacks were launched by Jundullah, a Sunni Islamist and Baluchi ethnic group.

2010: Kampala, Uganda attacks groups watching Football by Al-Shabaab (75)

In July 2010 Al-Shabaab attacked crowds watching a screening of the 2010 FIFA World Cup Final match at two locations in Uganda. The attacks left 74 dead and 70 injured. Al-Shabaab, claimed responsibility for the attacks as retaliation for Ugandan involvement in Somalia. This was Al-Shabaab's first attack outside of Somalia. The first bombing was carried out at a restaurant called the Ethiopian Village, with many of the 15 victims foreigners. The second attack, consisting of two explosions in quick succession, occurred at Kyadondo Rugby Club, with an explosion near the 90th minute of the match, followed seconds later by a second explosion, in total killing an estimated 50 persons. This attack was also likely carried out by suicide bombers and targeting non Muslim expatriates, though most of the dead were in fact Ugandan.

2010: Bombings in Abuja, Nigeria by MEND (12)

The Movement for the Emancipation of the Niger Delta (MEND) launched attacks beyond the Delta, in the capital, Abuja when it exploded a car bomb in the

city that killed 12. These bombings took place during celebrations for the country's 50th anniversary of independence.

2011: Oslo Bombing/Shootings, Norway by Far Right Extremist (77)

Anders Behring Breivik, an anti-Muslim, far right wing Christian fundamentalist planted a bomb in Oslo near the Prime Minister's Office killing 8 people. He then went to an island retreat for young members of the ruling Labour Party and shot and killed 69 teenagers, to draw attention to his far right anti Islamic views.

2011: Attacks in Nigeria by Boko Haram (105)

On the 4th of November at least 65 people lost their lives to a series of coordinated gun and bombs attacks in the Nigerian city of Damaturu. The attacks were believed to have been perpetrated by an Islamist sect known as Boko Haram, which launched an insurgency campaign against the Nigerian government in 2009. The name Boko Haram, which denotes "Western education is forbidden", expresses the sect's desire to impose Sharia law across Nigeria. On the 25 December 2011 Boko Haram carried out further bombings that killed almost 40 people.

2011: Attacks in Mogadishu against the transitional govt by Al Shabaab (45)

Whilst Islamist militant group Al-Shabaab controls much of the central and southern areas of the country it struggles with Transitional Federal Government that controls the capital, Mogadishu. Amongst the worst incidents in the city were armed attacks by Al-Shabaab in February and March 2011, which killed 21 and 24 respectively.

2011: Attack in Jonglei province, South Sudan, by SPLA offshoot (111)

Following the country's formal secession from Sudan in July 2011, South Sudan, violence has continued with a splinter group from the mainstream Sudan People's Liberation Army, led by George Athor, was responsible for 111 deaths in an attack in Jonglei province.

2012: Multiple bombings in Kano, Nigeria by Boko Haram (178)

At least 25 bombings and armed attacks occurred in Kano, Nigeria, killing at least 178. The attacks were attributed to Boko Haram, an Islamic terrorist group in Nigeria who targeted government offices causing explosions and entering into gun battles with the Police.

2012: Bombing in Sana'a, Yemen by Ansar al-Sharia (Al-Qaeda AP affiliated) (120)

The Sana'a bombing constituted an attack against Yemen army soldiers practicing for the annual Unit Day military parade on the 21st of May 2012. The attack claimed more than 120 lives, and as such was the deadliest in Yemini history. Responsibility was claimed by Al-Qaeda in the Arabian Peninsula (AQAP) affiliated

Ansar al-Sharia.

2012: Southern Yemen suicide bombing by AQ AP (45)

The bomber, suspected of being a member of Al-Qaeda in the Arabian Peninsula (AQAP), struck during a funeral service attended by members of civilian militias that helped the Yemeni Army in a campaign to recapture the town of Jaar from AQAP militants in June 2012. The suicide bomber killed 45 and injured 40. The US now consider the Yemeni branch of AQAP to be the most dangerous in the terrorist network. American advisers have been helping Yemen's military in its campaign, and Yemenis say the US has been carrying out drone strikes against the militants.

2013: Syrian Government accused of rocket attacks in Aleppo, Syria (82)

One of the largest losses of life in the Syrian Civil War occurred in January 2013 when two large explosions struck an area between the Aleppo University halls of residence and the faculty of architecture, killing 82 and injuring 160 more as students were gathering for the first day of exams. Syrian opposition claim the attack came from government jets that had targeted and bombed the campus.

2013: Attack on Algerian Gas facility by Al-Qaeda in the Islamic Maghreb (AQIM) (40)

In Aména, Algeria Al-Qaeda in the Islamic Maghreb (AQIM) linked terrorists under the command of Mokhtar Belmokhtar took more than 800 people hostage at a remote gas facility in Algeria. After a tense 4-day standoff with the Algerian Army and at least 2 assaults, the crisis ended, with at least 40 hostages and 29 militants confirmed dead, while 685 Algerian workers and 107 foreigners were freed.

2013: Suspected Boko Haram shootings over 3 days (31)

Boko Haram murdered 31 people over the course of 3 days, including 18 hunters selling bushmeat, who were shot at market in Damboa on January 21. Five people were shot in Kano on the next day as they were playing board games, and at 8 civilians were killed in Maiduguri on January 23, as gunfire was reported from parts of the city.

2013: Lashkar-e-Jhangvi bombings in Quetta and elsewhere in Pakistan (126)

A string of bombings hit Pakistan, killing 126 and leaving more than 240 people injured. A bombing at a crowded market in Quetta killed 12 and injured 47 in an attack claimed by the Balochistan separatist group, Lashkar-e-Jhangvi and later, twin blasts took place in quick succession at a snooker hall where a total of 92 people were killed in these attacks, including 9 policemen, 25 rescue workers and 3 journalists. In addition, an explosion at a Tableeghi Jamaat seminary in the Swat Valley, killed 22 people and wounded 60.

2013: Attack on Christian Church in Peshawar, Pakistan by Pakistani Taliban - TTP Jandullah (81)

In one of the deadliest attacks ever on the Christian community in Pakistan, a splinter group from the Pakistani Taliban attacked the All Saints Church of Pakistan, in Peshawar, about 120 kilometers (75 miles) from the country's capital, Islamabad. A congregation of about 500 people was attending the church, when 2 suicide bombers entered the church compound from the main gate and blew themselves up in the middle of the people. The All Saints Church was built in 1883 inside the old walled city of Peshawar. It was built to resemble a mosque from the outside, not for security reasons but to symbolize unity. Christians make up less than 3% of the Pakistani population of 193 million. Militant groups have also targeted other minorities including Shiite Muslims, who are significantly outnumbered by Sunnis in Pakistan. A splinter group of the Pakistani Taliban claimed responsibility for the church attack, blaming the US programme of drone strikes in tribal areas of Pakistan. "Until and unless drone strikes are stopped, we will continue to strike wherever we will find an opportunity against non-Muslims," said Ahmed Marwat, a spokesman for TTP-Jandullah. The main Pakistani Taliban, known as Tehrik-e-Taliban Pakistan (TTP), distanced itself from the attack. "We refuse to take responsibility for the church blast. This is an attempt to sabotage peace talks between the TTP and the government," said a TTP spokesman. Earlier this month, Pakistani officials announced plans to pursue peace talks with Taliban militants and withdraw troops from parts of the volatile northwestern region, which borders Afghanistan. Pakistani Prime Minister, Nawaz Sharif's released a statement stating that terrorists have no religion and targeting innocent people is against the teachings of Islam and all religions.

2013: Kenyan Shopping Centre attack by Al-Shabaab (67)

The attack by Al-Shabaab terrorists at the Westgate Mall in Westlands, 3kms (1.8 miles) northwest of Nairobi's city center, started at about 12:30 p.m. On Saturday 22 September as the Mall filled up. Middle class Kenyans and expatriates frequent the shopping center, which has more than 80 shops including bank outlets, a movie theater, casino, restaurants and a children's play area. Two explosions were heard within about five minutes of each other when the attack started, forcing panicked shoppers to seek shelter including in the parking area on the roof of the four-story building. The attackers, who threw grenades, told Muslims they could go free and that non-Muslims were the target. The Al-Shabaab terrorists entered through the main door of the mall and went on a shooting rampage, moving from the ground level to upper floors, initially killing 59 and injuring at least 175. The death toll later rose to at least 67 confirmed killed in the assault by 12 to 15 Al-Shabaab militants including 61 civilians and 6 security force personnel. Five militants also were killed, but questions remained about the fate of the remaining attackers and

fears persist that some had managed to escape. The raid was the deadliest attack in Kenya since the 1998 bombing of the US Embassy in downtown Nairobi that killed 213 people. The Al-Shabaab Islamist militant group in neighboring Somalia threatened to carry out attacks in Kenya after the country deployed its army to southern Somalia in October 2011 to fight the group. In 2010, the militants killed 74 people in an attack at a restaurant and sports club in Uganda. The Kenyan President Kenyatta vowed to hunt down the perpetrators of the attack and said he lost a nephew and his nephew's fiancee in the assault. Al-Shabaab, meanwhile, threatened more attacks in Kenya, stating on its Twitter feed that the mall attack "was just the premiere of Act 1." "Make your choice today and withdraw all your forces," the group's leader, Ahmed Abdi Mohamed Godane, said in a statement posted on the Internet late Wednesday. "Otherwise be prepared for an abundance of blood that will be spilt in your country, economic downfall and displacement."

2013: Nigerian College attack by Boko Haram (50)

A Nigerian College was attacked, in September, 2013 by Boko Haram in the dead of night, killing as many as 50 students as they slept in dormitories and torching classrooms, the latest in a series of Boko Haram attacks in Northern Nigeria as they continue their Islamic uprising. Boko Haram leader Abubakar Shekau has said in video addresses that his group wants to end democracy in Nigeria and allow education only in Islamic schools. Boko Haram means "Western education is forbidden." According to one witness, the terrorists, rode into the college in two pickup all-terrain vehicles and on motorcycles, some dressed in Nigerian military uniforms, who appeared to know the layout of the college, attacking the four male hostels but avoiding the one hostel reserved for women. Most schools in the area closed after earlier similar attacks including one in July that killed 29 pupils and a teacher. More than 30,000 people have fled to neighbouring Cameroon and Chad. The attacks come as Nigeria prepares to celebrate 53 years of independence from Britain and amid political jockeying in the run up to presidential elections next year.

2013: Attacks in Russia by Chechen Terrorists (Caucasus Emirates) (20)

Recent attacks have seen a series of terror attacks on buses, trains and airplanes, some carried out by suicide bombers, including in October 2013 a black widow suicide bomber who blew herself up on a city bus in Volgograd, killing 6 and injuring about 30 and another black widow suicide bomber who blew herself up at a railway station in Southern Russia, killing 14 and injuring scores more, heightening concern about terrorism ahead of February 2014 Olympics in the Russian Black Sea Resort of Sochi. The attacks have been claimed by the Caucasus Emirates.

See also Breaking News at the end of this Book.

Chronology of the World's Worst Airline Attacks by Terrorists

Whilst flying remains one of the safest forms of travel, incidents when they occur are more likely to result in fatalities. The first fatal aviation accident occurred in 1908, when Orville Wright crashed his Wright Model A aircraft during testing killing his passenger. It wasn't until 1933 that the first 2 Aeroplanes were destroyed intentionally first by fire and then by a bomb and is thought to be the first proven acts of air terror in the history of commercial aviation.

Passenger airliners as well as cargo aircraft have been the subject of plots or attacks ever since.

Many early bombings though were suicides or schemes for insurance money, but in the latter part of the 20th century, political and religious militant terrorism became the dominant motive for attacking large jets, either by hijacking, to publicize a cause or to make demands or by bombing to cause mass casualties. Whilst the political and religious motives are varied, many of the worst incidents, involve so called Islamic or Middle East Terrorists, from Pakistani based groups targeting India and supporting secession from India of Kashmir and Jammu provinces, Palestinian Groups fighting for their State, State sponsored terror from Libya, Chechens for Independence and Al-Qaeda for an Islamic Caliphate.

Whilst dynamite was first used, plastic explosive is the preferred form of bomb as it is both harder to detect and has greater explosive power. Whilst the most common form of terrorist attack was carried out by smuggling explosives into baggage, detonating the bomb once the plane is in the air usually by timers, more recently with Al-Qaeda representing the most active threat the modus operandi has changed. Al-Qaeda have attempted numerous new ways of bringing down airplanes, including using suicide bombers to either directly crash the planes or to explode bombs concealed by them or to carry on board chemicals which when mixed on board can produce an explosion. Most recently Al-Qaeda have targeted cargo planes with bombs

The deadliest aviation-related disaster of any kind, considering fatalities on both the aircraft and the ground, was the attack on America on 9/11/2001, killing almost 3,000 people.

The deadliest pure Aircraft disasters were not terrorist events. The first occurred in Tenerife when two Boeing 747 aircraft collided when a KLM Boeing 747 attempted take-off without clearance, and collided with a taxiing Pan Am 747 killing 583 people. The second

the crash of Japan Airlines Flight 123 in 1985 was the single-aircraft disaster with the highest number of fatalities. In this crash, 520 died on board a Boeing 747. The aircraft suffered an explosive decompression from an incorrect repair.

Whilst there are more than 85 cases related to airline bombings, with more than 50 of them resulting in deaths there are 14 cases resulting in 100 or more fatalities.

Worlds Worst Airline attacks by Terrorists (causing 100 or more fatalities)	
Deaths	Details
100	1973 - Aeroflot TU-104 exploded over Siberia after hijackers demands not met
100	1977 - A hijacked Malaysian Boeing 737 airliner downed
106	1993 - Transair Georgian Airlines TU-154B downed by a missile in Georgia by Abkhazian rebels
110	1989 - Avianca Flight 203 exploded in Colombia, Pablo Escobar responsible
112	2002 - China Northern Flight 6136 crashed in China after passenger suicide insurance attack
112	1983 - Gulf Air 771 Boeing 737 from Pakistan exploded in UAE downed by Abu Nidal Organisation
115	1987 - Korean Air Flight 858 downed by North Koreans
127	1996 - Ethiopian Boeing 767 crashed following hijacking by Ethiopians
132	1990 - Chinese Boeing 737 hijacked & crashed in China due to Chinese hijackers
171	1989 - French UTA Flight 772 DC-10 destroyed over Niger by Libyans
213	1999 - Egypt Air Boeing 767 crashed off Massachusetts after pilot intentionally downed it
259	1988 - Pan Am Flight 103 downed over Lockerbie, Scotland by Libyans
331	1985 - Air India Flight 182 from Montreal downed by extremist Sikhs
2997	2001 - Attack on America - 9/11 by AQ

Source: Author

The first recorded aircraft hijack took place in 1931, in Peru, when a pilot was approached on the ground by armed revolutionaries. Hijackings increased between 1948 and 1957, to 15 and between 1958 and 1967, this climbed to 48. There was an explosive increase to 38

in 1968 and 82 in 1969, the largest number in a single year in the history of civil aviation. During the period between 1968 and 1977, there were 414 hijackings and between 1988 and 1997, there were 180 hijackings and then from 1998 to 2007, 98. Since 2001 to the present day the numbers have fallen considerably to 43 incidents.

As far as hijackings are concerned perhaps the most well known occurred in 1976 of Air France 139 but not for the hijacking itself but for the daring raid by Israeli special forces who landed at Entebbe Airport, Uganda, and rescued 105 persons, almost all Israeli hostages killing all Palestinian hijackers (Popular Front for the Liberation of Palestine). However three passengers and one commando were killed.

From the 85 cases, the following 34 cases are perhaps the most shocking mass casualty events and/or of greatest importance, indicating new threats and/or targets or methods. Whilst the last decade has proven to be one where fatalities have been one of the lowest on record, this is due more to foiled and failed attempts, rather any reduction in threat levels.

The list is in chronological order and includes a brief summary for each case.

1933: Imperial Airways flight by passenger (15)

Imperial Airways flight over Belgium crashed probably after a fire started by a Passenger attempting to commit suicide, killing all 15 aboard. This is thought to be the first act of sabotage on a commercial airliner.

1933: United Airlines Boeing 247 by Chicago gangs (7)

United Airlines Boeing 247 was destroyed by a bomb, crashing near Indiana, USA, killing 7, thought to be the first case of airline sabotage by a bomb with nitroglycerine as the probable explosive. A Chicago gangland murder was suspected, but the case remains officially unsolved.

1949: Canadian Pacific Air Lines DC-3 by a Jeweller (23)

Canadian Pacific Air Lines DC-3 was destroyed by a bomb made of dynamite, carried onto the plane by the wife of the bomber leading to the death of all 19 passengers and 4 crew. A dynamite bomb was planted in the baggage compartment by a Jeweller, in a plot to kill his wife who was a passenger on the plane in order to collect US\$10,000 on an insurance policy. The Jeweler assembled the bomb, and his accomplices, one a clockmaker helped make the timing mechanism. All three were hanged for their crimes.

1955: United Airlines Flight 629 (44)

United Airlines Flight 629 was destroyed by a bomb containing dynamite in a suitcase carried by the bombers innocent mother after taking off from Denver on a

flight to Seattle. The explosion killed all 39 passengers and all 5 crew members. The bomber was executed for the pre-meditated murder of his mother who carried out the attack in order to collect US\$37,500 in insurance.

1959: National Airlines Flight 967 (42)

National Airlines Flight 967, Douglas DC-7B, the first jet airline to be downed when a bomb destroyed the aircraft over the Gulf of Mexico, killing 42. The bombing was carried on by a convicted criminal who was befriended and tricked by another man into boarding with luggage containing a bomb so that his wife would be able to collect on his life insurance.

1962: Continental Airlines Flight 11

Continental Airlines Flight 11 was a Boeing 707 aircraft which exploded while en route from Chicago to Kansas City. The following investigation focussed on one of the passengers, a married man with a five-year-old daughter, who had purchased a life insurance policy for US \$150,000, the maximum available; his death would also bring in another \$150,000 in additional insurance (some purchased at the airport) and death benefits. The bomber had recently been arrested for armed robbery and Investigators determined that he had also purchased six sticks of dynamite for 29 cents each, shortly before the crash. This was the first in-flight bombing of a jet airliner.

1966: Aden Airways DC3 (30)

Aden Airways DC3 was destroyed by a bomb enroute to Aden from the hill town of Maifa'ah, the capital of the Federation State of Wahidi, when it crashed into the desert. Investigations revealed a bomb had been placed on the instructions of Ali, the son of Amir Mohammed bin Said, Prime Minister of Wahidi who wanted to prematurely succeed him as Amir, who was killed together with 29 others on board.

1967: Cyprus Airways Flight 284 (66)

Cyprus Airways Flight 284 de Havilland Comet flying between Athens, Greece and Nicosia, Cyprus was destroyed leading to the plane crashing and the deaths of all 66 on board. A Greek general in command of the Cyprus army was the target of Turkish Terrorists, but the General cancelled shortly before departure.

1970: Swissair Flight 330 (47)

Swissair Flight 330 Convair CV-990 Coronado jet with 38 passengers and 9 crew members onboard crashed after a bomb exploded killing all on the aircraft. A barometric triggered IED had been used. Terrorism was suspected because of sentencing of three Palestinians by Swiss court and the Popular Front for the Liberation of Palestine allegedly claimed responsibility.

1973: Aeroflot Tu-104 (100)

Aeroflot Tu-104 exploded over Siberia en route from Moscow to Chita. The hijacker set off a bomb in the passenger cabin after his demands were not met, when

the plane was about 150km short of Chita, killing 100.

1976: Cubana Airlines (73)

Cubana Airlines plane exploded after takeoff from Barbados bound for Cuba. 73 people were killed and Cuban exiles in Venezuela were held responsible.

1976: Middle East Airlines Flight 438 (81)

Middle East Airlines Flight 438 exploded due to a bomb in the cargo bay of a Boeing 720B en route from Beirut, Lebanon to Dubai. The bombers were never identified. Lebanon was however going through a civil war at the time.

1976: Air France 139 (4)

Air France 139 was hijacked by the Popular Front for the Liberation of Palestine and the Plane was flown to Entebbe Airport, Uganda. Israeli special forces landed in secret at the Airport in Uganda, and rescued 105 persons, almost all Israeli hostages and killing all the hijackers. However three passengers and one commando were killed

1977: Malaysian Boeing 737 (100)

A hijacked Malaysian Boeing 737 airliner crashed near the Straits of Johore. The aircraft was descending when hijackers shot both pilots after which the airliner crashed in a swamp, killing all 100 aboard.

1982: Pan Am Flight 830 (1)

A Pan Am Flight 830 Boeing 747 was the target of a bomb attack. The bomb placed under a seat killed one 16 yr old Japanese boy injuring 15 more. The bomb was believed placed by a palestinian terrorist organisation.

1983: A Gulf Air Boeing 737 (112)

A Gulf Air Boeing 737 en route from Karachi to Abu Dhabi crashed after a bomb exploded in the baggage compartment. After the explosion, the plane crashed, killing 112 in the desert near Mine Jebel Ali in the UAE during an attempted landing. All 5 crew members and 105 passengers died. Most of the dead were Pakistani nationals, many returning to jobs in Abu Dhabi and Bahrain after spending the Eid al Adha holiday with their families in Pakistan. A passenger who checked in baggage at Karachi but never boarded the plane was held responsible and was a member of the Abu Nidal Organisation. The motive was believed to be extortion in trying to convince Gulf governments to pay protection money to Nidal so as to avoid attacks on their soil, including Saudi Arabia, Kuwait and the UAE.

1985: Air India Flight 182 (331)

Air India's Boeing 747 'Kanishka,' named after Emperor Kanishka who ruled an Indian state in the second century, cruised over the Atlantic at 31,000ft as it flew towards London, Heathrow. The aircraft, Flight 182, was on the east bound journey on a trip between India and Canada, via London. A large expatriate Indian community had settled in Canada and Flight 182 was over

three quarters full with 307 passengers of Indian origin. The large crew onboard the aircraft brought the total onboard to 329 people. Six thousand miles away on the other side of the world, ground staff at Tokyo's Narita Airport unloaded baggage containers from Canadian Pacific Air Lines Flight 003 which had recently arrived from Vancouver. As bags were being unloaded from a container, one piece of luggage exploded, killing 2 and injuring 4. Flight 003 from Vancouver, had arrived with a total of 390 people onboard, and had the aircraft been just half an hour the explosion would have caused a terrible disaster. Over the Atlantic, Air India Flight 182 would soon explode without warning killing all on board over the Atlantic Ocean whilst in Irish airspace. Both in Canada and Japan, a full-scale investigation of the Air India crash and the blast at Narita was being instigated by RCMP and Japanese police. An examination of passenger lists and computer records indicated that a traveller by the name of L. Singh had checked in at Vancouver but had failed to board Flight 003 to Tokyo's Narita Airport. Another M. Singh, had also checked in at Vancouver for a connecting flight to Sir India's Flight 182 but he had failed to turn up as well. In both instances their bags had been loaded. The investigation pointed to Sikh terrorists. Internal strife in the northern State of Punjab, brought about by extremist demands for a separate nation of Khalistan, had created civil unrest in India. The trouble came to a head in June 1984 in Amritsar with the Indian Army's storming of the Golden Temple, the Sikhs' holiest of shrines. The result was a bloodbath. Sikhs throughout the world were horrified by such an act. In retaliation, the Indian prime minister, Indira Gandhi, was assassinated by her own Sikh bodyguards. Her death stunned the world and created a Hindu backlash, which resulted in Sikhs being massacred in the streets of New Delhi. This bombing was in retaliation.

1986: TWA Flight 840 (4)

TWA Flight 840 a Boeing 727-231 flying from Rome's Fiumicino Airport to Athens, exploded ejecting four American passengers (including a nine-month-old infant) to their deaths and injuring five others. The bomb contained one pound of plastic explosive and was placed under a passenger seat by the Palestinian terrorist Abu Nidal Organisation.

1987: Korean Air Flight 858 (115)

Korean Air Flight 858 was brought down by liquid explosives concealed as liquor bottles by North Korean agents, who boarded the plane in Iraq and left in Abu Dhabi. The plane exploded en route to Bangkok over the Andaman Sea, killing all 115 abroad. The North Korean Agents were arrested in Bahrain but consumed poison concealed in cigarettes. The male died, but the female survived and later implicated North Korea, saying the bomb was planted to discourage people from attending the 1988 Seoul Olympics. This was the first known example of liquid explosives being used which would be taken up again in 1994, see Operation Bojinka below.

Special Focus 4 1988 - Pan Am Flight 103 (259)



On 21 December 1988, Pan American flight 103, took off from London, bound for New York City. A Boeing 747-121, named Clipper Maid of the Seas, was destroyed by Libyan Agents as it was climbing on its northerly flight path, exploding over the town of Lockerbie in southwest Scotland. In all, 270 people from 21 countries were killed, including all 259 passengers and crew members plus 11 people on the ground in Lockerbie. Many of the passengers came from the states of New Jersey and New York. The captain, first officer, flight engineer, a flight attendant, and a number of first-class passengers were found still strapped to their seats inside the nose section when it crashed in a field by a tiny church in the village of Tundergarth. The inquest heard that a flight attendant was found alive by a farmer's wife, but died before her discoverer could summon help. Two other passengers remained alive briefly after impact; medical authorities later concluded that one of these passengers might have survived if he had been found soon enough. This widely regarded assault on a symbol of the US, with 189 of the victims being Americans, stood as the deadliest terrorist attack on American civilians until the attacks of 11 September 2001.

On 5 December 1988 (16 days prior to the attack), a man with an Arabic accent had telephoned the U.S. Embassy in Helsinki, Finland, and told them that a Pan Am flight from Frankfurt to the US would be blown up within the next two weeks by someone associated with the Abu Nidal Organisation. The anonymous warning was taken seriously by the US government, and the State Department quickly informed all US carriers, including Pan Am. Whilst Pan Am had charged each of the passengers a US\$5 security surcharge, promising a "programme that will screen passengers, employees, airport facilities, baggage and aircraft with unrelenting thoroughness", the security team in Frankfurt found the warning under a pile of papers on a desk the day after the bombing.

In 1992 a US federal court found Pan Am guilty of wilful misconduct due to lax security screening. Alert Management Inc. and Pan American World Services, two subsidiaries of Pan Am, were also found guilty; Alert handled Pan Am's security at foreign airports. Largely as a result of this incident and the judicial findings, Pan

Am entered bankruptcy.

The motive that is generally attributed to Libya can be traced back to a series of military confrontations between Libya and the US which took place first in the 1980s in contested waters. First, there was a Gulf of Sidra incident (1981) when two Libyan fighter aircraft were shot down, then, two Libyan radio ships were sunk in the Gulf of Sidra, followed by the sinking of a Libyan Navy patrol boat and another Libyan vessel on 25 March 1986. It is believed that Muammar Gaddafi retaliated for these sinkings by ordering the 5 April 1986 bombing of West Berlin nightclub, La Belle, that was frequented by US soldiers and which killed three and injured 230 and in turn led to US President Ronald Reagan to launch military strikes against Libyan cities, Tripoli and Benghazi. The Libyan government claimed the air strikes killed Hanna, a baby girl Gaddafi claimed he adopted and to avenge his daughter's death, Gaddafi is said to have sponsored the September 1986 hijacking of Pan Am Flight 73 in Karachi, Pakistan. The US in turn encouraged and aided the Chadian National Armed Forces (FANT) by supplying satellite intelligence during the Battle of Maaten al-Sarra. The attack resulted in a devastating defeat for Gaddafi's forces, following which he had to accede to a ceasefire ending the Chadian-Libyan conflict and his dreams of African dominance. Gaddafi blamed the defeat on French and US "aggression against Libya". The result was Gaddafi's motive which led to Libyan support for the bombings of Pan Am Flight 103.

Despite many alternative claims for responsibility, Muammar Gaddafi finally admitted Libya's responsibility for the Lockerbie bombing. Gaddafi's admission followed a determined investigation over more than 11 years following which accusations and sanctions were made against the Libyan regime, though he maintained that he never personally gave the order for the attack. The UN which had made "accepting responsibility for the actions of its officials" among the steps set by the UN for lifting Sanctions against Libya. Other requirements included a formal denunciation of terrorism by Libya and compensation for the families of the PA103 victims. Libya offered compensation of up to US\$2.7bio to settle claims by the families, representing US\$10mio per family, with conditions. The Libyan offer was that 40% of the money would be released when UN sanctions, suspended in 1999, were cancelled; another 40% when US trade sanctions were lifted; and the final 20% when the US State Department removed Libya from its list of states sponsoring terrorism. In the end each family received US\$8mio (from which legal fees of about US\$2.5mio were deducted) and, as a result, the UN cancelled the sanctions that had been suspended four years earlier, and US trade sanctions were lifted. A further US\$2mio would have gone to each family had the US State Department removed Libya from its list of states regarded as supporting international terrorism, but as this did not happen by the deadline set by Libya, though it would be later removed in 2006 when full

diplomatic relations with Libya were resumed. Further settlements would follow for other incidents, including the 1986 Berlin discotheque bombing and in 2008, a US-Libya compensation deal was signed which covered 26 outstanding lawsuits filed by American citizens against Libya, and three by Libyan citizens in respect of the US bombing of Libya in 1986. Libya paid \$1.5 billion into a fund to be used to compensate relatives of victims. As a result, President Bush signed Executive Order 13477 restoring the Libyan government's immunity from terror-related lawsuits and dismissing all of the pending compensation cases in the US.

1989: French UTA Flight 772 (171)

A French UTA Flight 772 DC-10 was destroyed in mid-air over Niger by the explosion of a luggage bomb killing all 156 passengers and 15 crew members. The bomber loaded the bomb in Brazzaville, leaving the plane in N'Djamena, Chad, with the plane then scheduled to fly on to Paris. France indicted six Libyan Agents, including Abdullah Senussi, brother-in-law of Muammar Gaddafi, and deputy head of Libyan intelligence. Libya refused to extradite the six, who were condemned in absentia, but subsequently recognised its responsibility by compensating the families of the victims. The deemed motive of the bomber was revenge against the French for supporting Chad against the expansionist projects of Libya toward Chad.

1989: A Colombian Avianca Flight 203 (110)

A Colombian Avianca Flight 203, Boeing 727 passenger jet departing Bogota, Colombia, en route to Cali, exploded 5 minutes after takeoff under a passenger seat, causing the plane to crash, killing all 107 aboard as well as 3 on the ground. The bomb was planted by members of the Medellin Drug Cartel, led by Pablo Escobar, as part of the escalating war between the drug traffickers and the proponents of extradition to the US in Colombia. The motive was an assassination attempt on presidential candidate César Gaviria Trujillo, and an enthusiastic proponent of extradition, but the target was not on the flight. Trujillo would go on to win the 1990 presidential election. Two Americans were among the people seated on the plane, giving US President George H.W. Bush cause to supply new assets to the Colombian fight against the traffickers. It signaled the beginning of the end for Escobar, who would 4 years later be gunned down by Colombian special forces.

1990: Chinese Boeing 737 (132)

A Chinese Boeing 737 was hijacked during a domestic Chinese flight from Xiamen to Guangzhou. The Chinese hijacker claimed to have explosives and demanded the pilot fly to Taiwan. The pilot tried to persuade the hijacker that the plane held insufficient fuel for the extended trip and attempted an emergency landing in Guangzhou when his fuel levels became critical. Upon touching down, and during a fight in the cockpit between the hijacker and the pilot, the 737 swerved into two other aircraft on the ground, a Boeing 707 and a

Boeing 757, both China Southwest Airlines. The 737 overturned, killing 132 in total, 84 of 104 aboard and another 48 were killed on the 757.

1993: Transair Georgian Airlines Tu-154B (106)

Transair Georgian Airlines Tu-154B was hit by a missile while on approach to Sukhumi, Georgia. The aircraft crashed on the runway, killing 106 of 132 aboard. The missile was fired by Abkhazian Rebels.

1994: Philippine Airlines Flight 434 / Operation Bojinka (1)

Philippine Airlines Flight 434 was bound for Tokyo from Manila, but made an emergency landing at Okinawa, US after a blast ripped a two-foot-square portion out of the fuselage, killing one passenger and injuring 10. The bomb was made out of liquid explosives (nitroglycerin) packed into contact lens solution bottles and was made by Ramzi Yousef an Iraqi National, who also built and detonated the WTC 1993 bomb. This attack was in fact one of a number of tests Ramzi Yousef undertook with fellow plotter and Uncle, Khalid Shaikh Mohammed in furtherance of an ambitious planned large-scale three phase Islamist attack, called Operation Bojinka. The planned attacks involved a plot to assassinate Pope John Paul II, an air bombing of 11 airliners and their approximately 4,000 passengers that would have flown from Asia to the US, and a proposal to crash plane into the CIA's headquarters in Virginia, scheduled for 1995. Despite careful planning and the skill of Ramzi Yousef, the Bojinka plot was disrupted after a chemical fire drew the Philippine National Police's attention to the bombers apartment just a few days before the Pope's visit, where masses of evidence was found.

1996: An Ethiopian Boeing 767 (127)

An Ethiopian Boeing 767 passenger jet flying from Addis Ababa, Ethiopia, to Nairobi, Kenya, crashed during a hijacking. Three Ethiopian hijackers instructed the pilot to fly to Australia but the plane did not have enough fuel and was denied permission to land to refuel. The pilot brought the plane down a few hundred meters off a resort beach at Moroni in the Comoros Islands off Africa. The hijackers may have fought for control of the aircraft during descent, contributing to the crash during ditching. People on the beach were able to rescue 48 of the 175 aboard the plane, though 127 including the hijackers were killed.

1997: Malaysian Boeing 737 Flight 653 (100)

Malaysian Airlines 653 crashed in Malaysia killing 93 passengers and 7 crew, after reports that the flight had been hijacked. The downing though remains unsolved though some have speculated involvement of the Japanese Red Army.

1999: An Egypt Air Boeing 767 (217)

An Egypt Air Boeing 767 crashed off the coast of Massachusetts after departing New York City bound for Cairo, killing 217. The crash occurred 33 minutes after

takeoff near Nantucket Island, when the Egyptian relief first officer intentional crashed the aircraft. Flight data suggests that he shut off the engines and put the aircraft into a steep dive; a second crew member unsuccessfully struggled for control of the aircraft, which broke apart from aerodynamic stresses and crashed.

2001: Attack on America 9/11 (2,997)

For more details see [Special Focus 1 - Attacks on America \(9/11\)](#) earlier in this Part 2, Section 6.

2001: American Airlines Flight 63 (0) - the Shoe Bomber

American Airlines Flight 63 was bound for Detroit from London in December of that year and was the target of a failed Al-Qaeda bombing attempt. As Flight 63 was flying over the Atlantic Ocean, Richard Reid, wearing shoes that were packed with plastic explosives (PETN and TATP) tried to set these off with a match to a fuse leading into the shoe but he was spotted by flight attendants and with the aid of passengers tackled and eventually restrained. This incident led to changes in security protocols in US airports where passengers shoes must now be removed and screened.

2002: China Northern Flight 6136 (112)

China Northern Flight 6136, an MD-82 jetliner on a domestic flight from Beijing to the coastal city of Dalian was brought shortly after the pilot reported "fire on board", killing all 103 passengers and 9 crew members. A Chinese passenger set fire to the passenger cabin with gasoline, causing the plane to lose control and crash. This passenger had purchased seven air insurance policies worth a total of about US\$170,000 prior to boarding the flight.

2004: Volga-Avia Express Flight 1303 (89)

Volga-Avia Express Flight 1303, a Tu-134 aircraft and a Siberia Airlines Flight 1047, a Tu-154 aircraft both crashed in Russia within minutes of each other flying different routes. The first killed all 34 passengers and 9 crew members on board the plane and the second all 38 passengers and 8 crew members on board the plane. The two almost simultaneous crashes immediately caused speculations about terrorism. The following investigation found that the planes were downed by bombs triggered by two female Chechen terrorist suicide bombers. Shamil Basayev militant leader of the Chechen terrorist movement, the Islamic International Peacekeeping Brigade, claimed the credit. In an open letter he claimed that the aircraft bombings cost him US\$4,000 in total.

2006: 10 Airliner Atlantic Plot (0)

Attempted Al-Qaeda terrorist plot to detonate liquid explosives carried on board at least 10 airliners traveling from the UK to the US and Canada. It followed the same general plan as the Bojinka plot (see above). Individuals arrested in the UK and Pakistan planned to carry household chemicals and liquids in their carry-on luggage, but then mix them aboard the plane to make

small bombs. The bombs would have been powerful enough to create an explosive decompression aboard an aircraft causing the plane to disintegrate while flying at high altitude over the ocean. Had the attack been successful the estimated death toll could have exceeded the 3,000 killed on 9/11/2001.

2009: Northwest Airlines Flight 253 (0) - Christmas Day bombing / Underpants Bomber

On Christmas Day 2009, Abdulmutallab travelled from Ghana to Amsterdam, where he boarded Northwest Airlines Flight 253 en route to Detroit. He had a Nigerian passport and a valid US tourist visa and purchased his ticket with cash in Ghana on 16 December. Abdulmutallab, the youngest of 16 children of a very wealthy Nigerian banker, grew up a pious muslim, travelling to Yemen and then to the UK where he attended University College London in 2005 and earned a degree in mechanical engineering in 2008.

He was on the radar of MI5, the UK's domestic counter-intelligence and security agency and the CIA, though the CIA added the suspect's name in November 2009 to the US's 550,000-name Terrorist Identities Datamart Environment, a database of the US National Counterterrorism Center (NCTC). It was not added to the FBI's 400,000-name Terrorist Screening Database, the terror watch list that feeds both the 14,000-name Secondary Screening Selectee list and the US's 4,000-name No Fly List, nor was an existing Abdulmutallab's US visa revoked. On the flight, Abdulmutallab spent about 20 minutes in the toilet as the flight approached Detroit, and then covered himself with a blanket after returning to his seat. Other passengers then heard popping noises, smelled a foul odor, and some saw Abdulmutallab's trouser leg and the wall of the plane on fire. A fellow passenger jumped on Abdulmutallab and subdued him as flight attendants used fire extinguishers to douse the flames. The device consisted of a six-inch (15-cm) packet which was sewn into his underwear containing the explosive powder PETN, which became a plastic explosive when mixed with the high explosive triacetone triperoxide (TATP) (the same two explosives that were used by Richard Reid, the shoe bomber, in 2001 and a syringe containing liquid acid).

President Barack Obama immediately ordered a review of detection and watch list procedures. Saying that "totally unacceptable" systemic and human failures had occurred

Abdulmutallab was arrested. He would be later tried, plead guilty and was sentenced to 4 life sentences. Abdulmutallab told authorities he had been directed by Al-Qaeda in the Arabian Peninsula, and that he had obtained the device in Yemen.

Special Focus 5

2010 - UPS Flight 232 & FedEx Cargo Planes



UPS Flight 232 a Boeing 767 cargo plane and a FedEx Express cargo plane were due to carry packages across the Atlantic to the USA that included a Hewlett-Packard HP LaserJet P2055 desktop laser printer. Inside each printer was a sophisticated, expertly constructed bomb in its toner cartridge, which was filled with explosives. The toner cartridges were filled with the odorless military grade plastic explosive (PETN), a white powder that is one of the most powerful explosives known.

Each bomb also consisted of cell phone circuitry with an alarm timer, a phone battery, a thin wire filament, and a syringe filled with lead azide. The bombs' detonators were the alarm timers on cell phone circuitry that was discovered in the two bombs. Each bomb had a cell phone alarm that had been set, which was constructed to trigger power from a phone battery. That would in turn send an electrical current through, and heat, a thin wire filament, similar to those in light bulbs. The wire filament, from a broken light-emitting diode, was in a plastic medical syringe that contained 5 grams of lead azide, a powerful chemical initiator. Once hot, the lead azide would ignite. That would then cause the PETN to detonate.

The packages were intercepted in the UK and in Dubai being shipped in cardboard boxes that also for example contained souvenirs, clothes, compact discs, and several books written in English. Al-Qaeda in the Arabian Peninsula (AQAP) took responsibility for the plot, which was uncovered by Saudi Intelligence, tipping off UK, Dubai and US authorities.

According to the US and the UK, the bombs were probably designed to detonate mid-air, with the intention of destroying both planes over Chicago or another city in the US. Each bomb had already been transported on both passenger and cargo planes. The packages had already flown on earlier passenger and cargo planes to reach their current destinations, evading security checks. Despite the tip offs an initial search by anti terrorist officers, for example in the UK on one of the Cargo planes with explosive detection equipment and sniffer dogs, they failed to find any explosives.

When US authorities provided the precise tracking number of the package, the printer was scanned, x-rayed, subjected to chemical swabs, and sniffed by bomb-sniffing dogs. Still, no explosives were detected but it was removed and subjected to further analysis. Scotland Yard explosive officers separated and removed the printer cartridge from the printer during their examination, only then identifying the bomb and deactivating it with only 3 hours before the bomb was due to explode.

AQAP later provided a detailed account of the plot (which it called "Operation Hemorrhage") in its English-language magazine Inspire, said that it cost only US\$4,200 to mount and was intended to disrupt global air cargo systems, and said it reflected a new strategy of low-cost attacks designed to inflict broad economic damage. The magazine included photos of the printers and bombs, as well as a copy of the novel Great Expectations by Charles Dickens that it said it had placed in one package, because AQAP was "very optimistic" about the operation's success.

The importance of this case cannot be overstated for the following reasons:

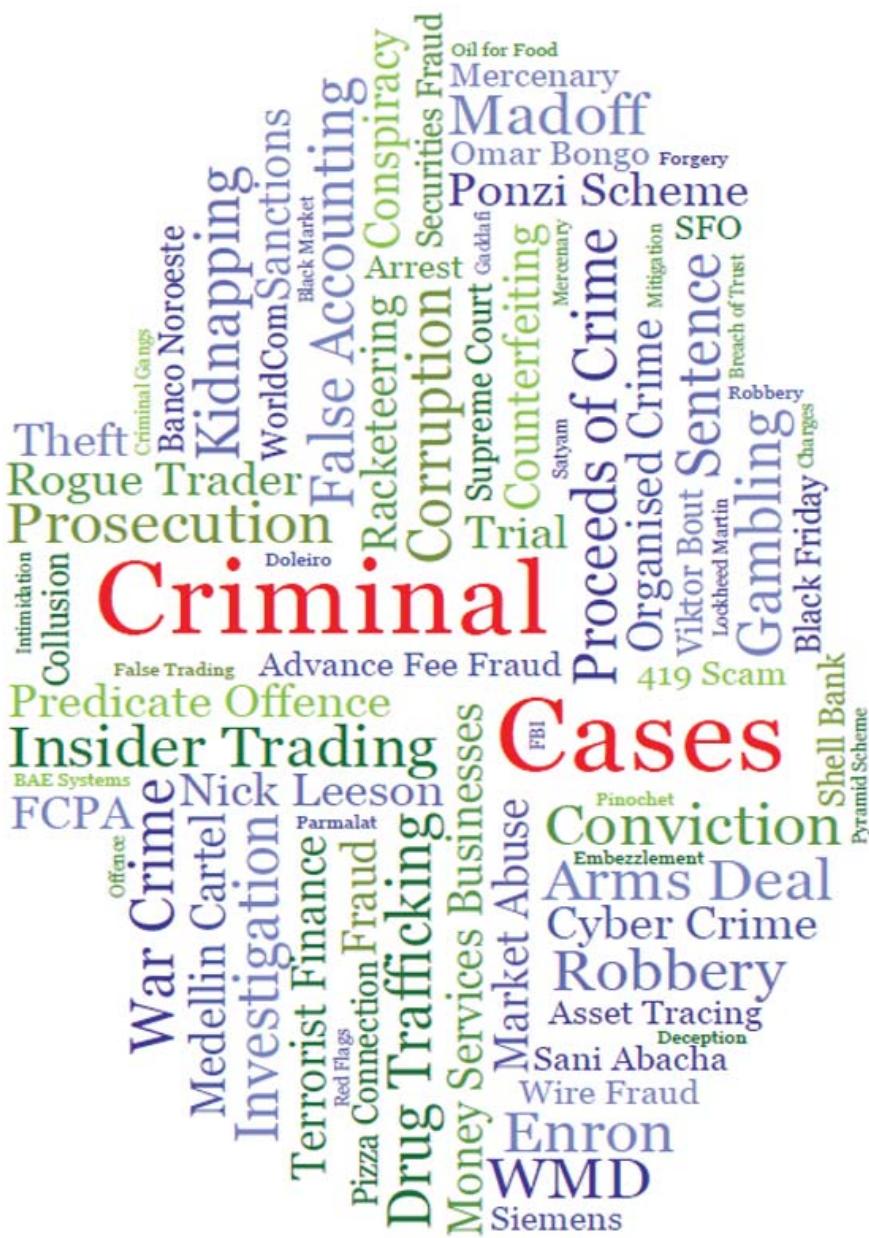
Both parcels in the 2010 cargo plane bomb plot were x-rayed without the bombs being spotted. Qatar Airways, that had unbeknown to it at the time had carried one of the bombs on board one of its passenger planes said the PETN bomb "could not be detected by x-ray screening or trained sniffer dogs".

The German authorities received copies of the Dubai x-rays, and an investigator said German staff would not have identified the bomb either.

Whilst many technologies can be used to detect PETN, a number of which have been implemented in public screening applications, primarily for air travel, this is much more difficult for Cargo. One technology, used for passenger flights, is where test swabs are wiped on passengers and their baggage for traces of explosives, though this is generally reserved for travellers who are thought to merit additional scrutiny.

A second type of machine, whole-body imaging scanners, use radio-frequency electromagnetic waves, low-intensity X-rays or T-rays of terahertz frequency to detect objects under clothing; but again these are used only on a limited basis and again only for passengers.

Section 7 - Criminals/Cases



- Introduction, 542
 - Corruption
 - Individuals / Politically Exposed Persons, 543
 - Ferdinand Marcos, 543
 - Special Focus 1 - Papa Doc & Baby Doc Duvalier, 543
 - Manuel Noriega, 544
 - Special Focus 2 - Raúl Salinas, 545
 - Mobutu Sese Seko, 547
 - Augusto Pinochet, 547
 - Special Focus 3 - Sani Abacha, 548
 - Pavel Lazarenko, 549
 - Slobodan Milošević, 550
 - Alberto Fujimori, 550
 - Vladimiro Montesinos, 551
 - Mohammed Suharto, 552
 - Joseph Estrada, 553
 - Paulo Maluf, 553
 - Arnoldo Alemán, 554
 - Frederick Chiluba, 554
 - Saddam Hussein, 555
 - Ali Zardari - Bhutto, 556
 - Teodoro Obiang & Son, 556
 - Diepreye Alameyeseigha, 557
 - Special Focus 4 - Randy "Duke" Cunningham, 557
 - Special Focus 5 - Omar Bongo, 558
 - Zine El Abidine Ben Ali, 558
 - Muammar Gaddafi & Son, 559
 - Muhammad Hosni Mubarak, 560
 - James Ibori, 560
 - Corporates, 561
 - Lockheed Martin, 561
 - Bofors, 561
 - Special Focus 6 - Thomson CSF -Thales, 562
 - Statoil, 563
 - BAE Systems, 564
 - Special Focus 7 - Siemens, 565
 - Kellogg Brown & Root, 566
 - Macmillan Publishing, 567
 - Special Focus 8 - GlaxoSmithKline, 567
 - Environmental Crime, 568
 - Seveso, 568
 - Bhopal, 568
 - Chernobyl, 568
 - Fraudsters, 569
 - Accounting Fraudsters, 569
 - Alan Bond, 569
 - Robert Maxwell, 569
 - Others, 610
 - Douglas Jackson, 610
 - Pokerstars & Others, 611
 - Advance Fee Fraudsters, 581
 - Special Focus 10 - Chief Nwude & Banco Noroeste, 581
 - Hassan Ali Khan, 581
 - Hedge Fund/Investment Co Fraudsters, 582
 - Jordan Belfort, 582
 - Michael Brown, 582
 - Samuel Israel III, 583
 - Special Focus 11 - Berni Madoff, 583
 - Sammy Goldman & Harry Tanner Jr , 585
 - Ponzi - Pyramid Schemes, 586
 - Special Focus 12 - Charles Ponzi, 586
 - Special Focus 13 - Ivar Krueger, 587
 - Barry Minkow, 587
 - Rogue Traders, 588
 - Special Focus 14 - Nick Leeson, 588
 - Toshihide Iguchi, 590
 - Kyriacos Papouis, 592
 - Peter Young, 593
 - Yasu Hamanaka, 593
 - Joseph Jett, 595
 - John Rusnak , 596
 - Liu Qibing, 599
 - David Lee, 599
 - Jerome Kerviel, 601
 - Frances Yung, 603
 - Kweku Adoboli, 604
 - Private Banker Fraudsters, 606
 - Hans Peter Walder, 606
 - Tax Fraudsters - Tax Evaders, 607
 - Mikhail Khodorkovsky, 607
 - Operation Wickenby, 608
 - Pasquattro Brothers, 609

- Insider Traders, 611
- R Foster Winans, 611
- Special Focus 15 - Ivan Boesky & Others, 612
- George Soros, 613
- Special Focus 16 - Ernest Saunders, 614
- James McDermot Jr, 615
- Martha Stewart, 615
- Philippe Jabbé, 616
- Anthony Elgindy & Others, 616
- Michael Guttenberg & Others, 617
- Takafumi Horie, 617
- Chen Rongsheng, 618
- Chris Littlewood & Others, 618
- Nicos Stephanou & Others, 619
- Stanko Grmosek, 619
- Mehmet Sepil, 620
- Special Focus 17 - Raj Rajaratnam, 620
- Malcolm Calvert, 622
- Oswyn Indra de Silva, 622
- John Hartman, 622
- Winifred Jau & Others, 623
- Joseph Skowron, 623
- US Congress, 624
- David Einhorn & Others, 624
- SAC Capital , 624

- Kidnappers / Robbers / Extortioners / Forgers, 625
- Elmyr de Hory, 625
- Gerd Heidemann, 625
- Glico-Morinaga, 625
- Special Focus 18 - Northern Bank / IRA, 626
- Special Focus 19 - Ingrid Betancourt, 627
- The History Men, 628
- Kiyoshi Takayama, 629

- Market Abusers, 629
- Tulip Bubble - 1634, 629
- South Sea Company, 630
- William Duer, 631
- London Stock Exchange Hoaxers of 1814, 632
- NY State Senator Kimble - 1840s, 632
- Daniel Drew & Others, 632
- Special Focus 20- Stock Market Crash 1929, 633
- Michael J Meehan, 634
- Albert H Wiggin, 634
- Charles Mitchell, 634
- Richard Witney, 634
- The Hunt Brothers, 635
- Special Focus 21 - Michael Milken, 635
- John Kaweske, 637
- The Flaming Ferraris, 637
- California Electricity Crisis, 638
- Shell, 639
- Ken Mahaffey & Others, 639
- Simon Eagle, 640

- Christopher McQuoid, 640
- Dipak Patel & Others, 640
- David Mason, 641
- Christopher Pia, 641

- Traffickers, 642
- Illicit Arms Traffickers, 642
- Basil Zaharoff, 642
- Adnan Khoshoggi, 643
- Leonid Minin, 643
- Simon Mann, 644
- Mohamed al-Kassar, 645
- Tomislav Damjanjanovic, 646
- Pierre Falcone, 646
- Special Focus 22 - Victor Bout, 647

- Drug Traffickers (Organised Crime), 649
- The French Connection, 649
- Special Focus 23 - Pizza Connection, 649
- La Mina/Operation Polar Cap, 650
- Special Focus 24 - Lucy Edwards & Peter Berlin, 652
- Speed Joyeros, 653
- Beacon Hill, 653
- Lespan, 653
- Special Focus 25 - Pedro Allatore, 654

- Goods Traffickers, 655
- Operation Pangea & Others, 655
- Human Traffickers, 656
- Robert Mikelsons, 656
- Operation Bia & Others, 656

- Terrorism Financiers, 658
- International Islamic Relief Org (Philippine & Indonesian Branches) (IIRO), 658
- Special Focus 26 - Holy Land Foundation, 658
- The Benevolence International Foundation (BIF), 659
- Muwafaq Foundation or "Blessed Relief", 660
- Al-Rashid Trust, 660
- The Rabita Trust, 660
- Special Focus 27 - Al Haramain Islamic Foundation (Bosnian & Serbian Offices), 661
- The Afghan Support Committee/Revival of Islamic Heritage Society, 661
- Global Relief Foundation, Taibah International and Al Furqan, 661
- Special Focus 28 - Interpal & Others, 662
- Carnival French Ice Cream, 662
- al-Aqsa Foundation, 663
- Al-Akhtar Trust, 663
- Sanabul Charitable Committee, 663

- WMD Proliferation Financiers/Sanctions, 664
- Ummah Tameer-e-Nau, 664
- Special Focus 29 - Abdulrahman Alalamoudi, 664
- Special Focus 30 - Abdul Qadeer Khan, 666
- Karl Lee, 668

Introduction

The supposed response from former UK Prime Minister, Harold Macmillan when asked what a prime minister most feared; "Events, dear boy, events"¹ was meant to be a comment about "big and unexpected" things happening.

The remark could equally be applied to those dealing in the money laundering prevention area as new events often shape the future money laundering landscape, priorities and the nature of the debate and responses following the occurrence of such events, perhaps, particularly illustrated by the events of 9/11 and Al-Qaeda's attack on America.

Perhaps a further quote is also relevant being that made by US Secretary of Defence, Donald Rumsfeld in 2002 in the aftermath of 9/11, when he said "There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say, we know there are some things we do not know. But there are also unknown unknowns the ones we don't know we don't know".²

In taking a closer look at more than 150 of the most infamous or if you prefer celebrated AML cases, the known knowns if you will, we can build a picture of many of the events that have shaped the money laundering landscape over the last decades and shaped the thinking, design and activity behind a Financial Institutions AML programme. We can also identify the criminal modus operandi in this instant. Whilst it is tempting to assume any particular case example can act as a proxy for a typology, it is both lazy and dangerous to do so. Nevertheless, in looking in detail across Cases, those that we have and where important connections can be made we can begin to see patterns and common elements that indicate risks which warrant greater focus, care and attention, if you will, that provide us with insight for future known unknowns.

These cases have been selected to showcase examples of the predicates, customer, products and services, channels and country risks and their respective interplays. Current money laundering programmes are designed to combat cases where history could be repeated, though no programme is infallible, is subject to human and other error, no two cases are ever the same and looking to the past will not enable us to predict the future.

The only sure certainty is that "Events dear boy events, will continue to ring true and these Cases will surely require supplementing with new Cases, no doubt some

falling into the category of known knowns, some known unknowns, becoming known knowns and as for the unknown unknowns that's life!

In this Part 2, Section 7, over 150 important cases are summarised with 30 given special attention with detailed profiles provided. Areas comprehensively covered and focussed upon include the most important predicate crimes, including corruption, for example, by Kleptocrats and PEPs, by companies paying bribes; by fraudsters ranging from those in the Corporate boardroom, rogue traders in investment banks, Ponzi schemers and other investment type fraudsters; by insider dealers, market abusers, kidnappers, extortioners and forgers, illicit arms traffickers, drug traffickers and organised criminals, goods and human traffickers, terrorist financiers, WMD proliferators and sanctions busters.

Corruption Individuals/PEPs

Ferdinand Marcos

Ferdinand Marcos was President of the Philippines from 1965 to 1986. President Marcos initially rose to power with widespread popular support and much was done to improve the economic situation faced by the Country though this became marred by high levels of corruption. As his health deteriorated his wife, Imelda, rose to prominence and assumed primary control over the country and its assets. By 1984, the US which had provided significant support to the Marcos regime began to distance itself from the regime and President Carter began an increasing campaign of public comment and criticism. In the light of this, Marcos decided to call an election but was defeated when the opposition parties combined to support the election of Corazon Aquino the widow of the prominent opposition leader that Marcos was alleged to have conspired to have murdered in September 1983. Marcos fled into exile in February 1986 and it was only then that the true extent of his corruption and abuse of power became evident.

US Customs Agents discovered 24 suitcases of gold bars as well as significant quantities of diamonds and currency and, as was widely publicised, it was discovered that his wife had over 2,500 pairs of shoes in the presidential mansion. Switzerland blocked assets in early 1986 upon the first signals that Marcos may try to siphon off money from Switzerland. Marcos died in Honolulu on 28 September 1989 and this was the catalyst for numerous actions to be started from individuals who sought restitution and return of funds stolen by the regime.

Imelda Marcos was subsequently tried in the US for embezzlement in 1990 but acquitted. In 1995 thousands of Filipinos won a class action against the Marcos estate in the US seeking damages for victims or relatives of victims of the regime but this action was dismissed.

Actions to trace and return the assets to the Philippines have been ongoing ever since and the nature and complexity of the structures and methods by which the funds were moved makes it extremely difficult for investigators to locate them with billions of dollars estimated taken from the Treasury and moved to accounts held offshore often in the names of "front companies". Some success has been achieved in this regard with the Swiss government returning US\$684mio. According to Transparency International in 2004 he was the second most corrupt leader who stole funds of around US\$5-10bio.

Country: Philippines
Key date: 1986 (fled into exile in Hawaii)

Special Focus 1 Papa Doc & Baby Doc Duvalier



Francois Duvalier (known as Papa Doc) was the President of Haiti from 1957 to 1971. He trained as a doctor and subsequently specialised in fighting tropical diseases which ravaged the poorer segments of the Haitian population. This work was to first bring

him to public prominence and helped result in him being known as "Papa Doc". He subsequently served as Director of the National Public Health Service. In 1949 he was forced to go into hiding as a result of a military coup. A succession of provisional governments followed but Duvalier finally gained the Presidency in 1957. Whilst his early years weren't particularly corrupt the later years in office was when he misappropriated millions of dollars in international aid with the funds being moved off the island and into accounts held in his name and the names of his family in a variety of other jurisdictions. In addition, he used his position to obtain official loans from other countries which he then promptly took for his personal use. Corruption became endemic and included extortion of local businesses and industries and created a situation where bribery was essential if anything associated or dependent on a government agency or department was going to progress. The government seized land from farmers and awarded them to those in the military and militia who supported Duvalier and famine and malnutrition spread widely.

Duvalier held power until his death in early 1971 and was succeeded by his son Jean-Claude who became known as "Bebe Doc". He made some token gestures such as releasing political prisoners but in reality opposition continued not to be tolerated and was frequently eliminated.

Like his father before him he abused his position and the finances of the country exploiting his near monopoly of the tobacco industry to generate considerable profits for himself and his direct family. He married in 1980 and through a combination of factors, including the vast expense of the ceremony which exceeded US\$3mio, further alienated the population

which was already suffering from a spread of AIDS which had, in turn, dramatically reduced tourism levels in the country. In 1983, Pope John Paul II visited Haiti and declared that "something must change here". This, combined with comments from other international observers, triggered a revolt in 1985 which included demonstrations and raids on government offices and storage facilities. This led to a series of measures by Duvalier which included deployment of the military, huge rises in the price of food and restrictions on the media.

In 1986 the US began to pressure Duvalier to leave and he finally left for France in 1986 transported in a US military aircraft. In France, Duvalier lived the high life in a plush villa, shopping at jewellers and vacationing at ski resorts, then gradually ran out of money after his wife divorced him in 1993 and was eventually placed under house arrest.

In his 15 years in power, Baby Doc and his glamorous wife, Michele Bennet, stole an estimated US\$500mio from the Haitian treasury, mainly through the president's "non-fiscal account" at the Regie du Tabac, the Haitian government's Tobacco Administration. Apparently the Duvaliers lived an expensive life in France; when the French authorities once raided their house in the South of France and seized a notebook from Mrs Duvalier. It showed some of her expenses from a recent shopping trip. They included US\$168,000 for clothes at Givenchy, US\$270,000 for jewellery at Boucheron, US\$9,752 for two children's horse saddles at Hermes, US\$68,500 for a wall clock and US\$13,000 spent for a week's stay at a Paris hotel. When the Duvaliers divorced in 1993, and Baby Doc was left apparently with little money for himself.

In 1986, The new Haitian government made a request for mutual legal assistance to Switzerland. Several accounts held by the Duvaliers in Switzerland were then frozen. These seizures included an account (approx US\$4mio) held by the Brouilly Foundation (incorporated under the laws of Liechtenstein), whose beneficiary was Simone Ovide Duvalier (the wife of Papa Doc). Over the course of the next 14 years, the court would be challenged by the legal claims from the Duvalier family to the money and Haitian government resistance to charging Baby Doc with any crimes in Haiti, which was a pre requisite under Swiss law to allow the Swiss to take the monies and provide it to the Haitian government. As a way out, the Swiss government had proposed giving the money to aid groups working in Haiti but in 2011, the Swiss Supreme Court whilst stating its unhappiness at the decision ruled that due to the Statute of Limitations it

could no longer object to the assets being claimed by the Duvaliers. It urged lawmakers to make it easier for assets belonging to deposed dictators to be repatriated to national governments and taking up this request Swiss lawmakers did just that passing the so-called "Duvalier law". The legislation was designed to open the way for the return of the funds, frozen in Swiss bank accounts during years of legal argument and efforts by Duvalier to reclaim them. In May 2011, the Swiss government started proceedings to return these assets (now US\$6.7mio) to the government of Haiti.

In January, Duvalier unexpectedly returned to Haiti after 25 years of exile in France, saying he wanted to help his compatriots rebuild after the huge earthquake that killed more than 300,000 people a year before. Since his return to Haiti, he has been charged with corruption, embezzlement and other abuses of power. Authorities have confiscated his passport. According to Transparency International in 2004 Papa Doc was the sixth most corrupt leader who stole funds of US\$300-800mio.

Position: Presidents of Haiti

When: 1957-1971 / 1971-1986

Amounts Involved: US\$300-800mio

Country: Haiti

Key date: 1986 (Baby Doc fled Haiti)

Manuel Noriega

President Manuel Noriega (also known as Pineapple face to his detractors) was infamous as the man who was the de facto military dictator of Panama from 1983 to 1989. Noriega worked with the CIA and US Army and became a paid intelligence agent since at least 1966 until 1986. In fact from 1978 until 1987, Noriega received numerous letters of appreciation from US officials for his cooperation in combating drug trafficking, for example, from Attorney General William French Smith in 1984 and DEA Administrator John C. Lawn in 1987. However by 1988 the US Senate Subcommittee on Terrorism, Narcotics and International Operations announced that: "The saga of Panama's General Manuel Antonio Noriega represents one of the most serious foreign policy failures for the US. Throughout the 1970s and the 1980s, Noriega was able to manipulate US policy toward his country, while skillfully accumulating near-absolute power in Panama. It is clear that each US government agency which had a relationship with Noriega turned a blind eye to his corruption and drug dealing, even as he was emerging as a key player on behalf of the Medellin Cartel a member of which was notorious Colombian Drug lord Pablo Escobar". They then went on to say that Noriega was allowed to establish "the hemisphere's first 'narcoleptocracy'". Noriega, in effect sold his government to drug traffickers for millions of dollars in bribes and turned Panama into a centre of international cocaine smuggling. US

prosecutors suggested a clear connection between Noriega and the Medellin Colombian drug cartel that was responsible for more than half of the cocaine smuggled into the US, in particular for example by receiving millions of dollars in payoffs. The US invaded Panama in December 1989 arresting and taking Noriega as prisoner to Miami. He stood trial and in 1992 was convicted of drug trafficking, money laundering and racketeering. His sentence was reduced from 30 to 17 years for good behaviour and he was released and then extradited to France in September 2007. In Paris in 2010, a Court sentenced him to 7 more years, but later in 2011 as the result of a request from Panama, France agreed to extradite Noriega to Panama so he would face trial for human rights violations and be convicted and sentenced to three 20-year sentences for crimes committed during his notorious 1983-1989 regime.

Country: Panama

Key date: 1989 (US invasion of Panama and arrest of Noriega)

Special Focus 2

Raúl Salinas



Raúl Salinas is the brother of former President of Mexico Carlos Salinas. He is best known for all the wrong reasons, being convicted of arranging the killing in 1995 of his former brother-in-law, although he was acquitted upon appeal in 2005, and being the focus of US

Senate hearings which claimed that he had laundered over \$90 million out of Mexico via the US and into private bank accounts in London and Switzerland, between 1992 and 1994, being largely the proceeds of corruption and/or receipts from the Mexican criminal gangs involved in the drug trade.

Carlos Salinas was elected (though claims of election fraud abound) Mexican President in 1988 and served until 1994 as the nominee of the Institutional Revolutionary Party (PRI) that had won all presidential elections since its inception in 1929. The corruption associated with the Salinas Presidency and the activities of Raúl Salinas were influential in the shift away from one party rule, as Mexicans looked for political reform that would eliminate the potential for similar abuses.

In November 1995, Raúl Salinas' wife, Patricia Salinas and her brother Antonio Castañón were arrested in

Geneva, Switzerland after attempting to withdraw US\$84mio from accounts believed to be beneficially owned by Raúl Salinas.

A report by the US General Accounting Office led to hearings in the US Senate which highlighted that Raúl Salinas transferred over US\$90mio out of Mexico and into private bank accounts in London and Switzerland, through a complex set of transactions between 1992 and 1994, via Citibank and its affiliates. In 2008, the government of Switzerland turned over US\$74mio, out of the US\$110mio in frozen bank accounts held by Raúl Salinas, to the government of Mexico. The Swiss Justice Ministry indicated that the Mexican government had demonstrated that US\$66mio of the funds had been misappropriated, and the funds, with interest, were returned to Mexico. The money was wired by and through Citibank offices to bank accounts held at Citibank in Zurich but assets were also identified at Pictet & Cie, Julius Baer Bank, Banque Privée and Edmond de Rothschild in Geneva and Zurich. Other funds were returned to third parties, including Mexican billionaire Carlos Peralta Quintero, who had given the funds to Raúl Salinas to set up an investment company.

According to the US government, the US report also made criticisms about other Citibank private banking accounts held by the sons of Nigeria's late military dictator Sani Abacha, Asif Ali Zardari, the husband of former Pakistani Prime Minister Benazir Bhutto and future Pakistani President and the President of Gabon, Omar Bongo. The US Senate focussed however mainly on the Salinas relationship, claiming that from 1992, Citibank assisted Salinas with transfers out of Mexico effectively disguising the funds' source and destination, thus breaking the funds' paper trail. Citibank according to the US government first opened a checking account in New York under Mr Salinas' name. This was then replaced with a complex structure of Companies, established by Citibank in the Cayman Islands. First an offshore private investment company named Trocasa Private Investment, Co. was established. The Directors of Trocasa were 3 separate Citibank Cayman nominees companies, Madeline Investment SA, Donat Investment SA, and Hitchcock Investment SA. Trocasa's officer and principal shareholder was another company formed by Citi Cayman named Tyler Ltd. Further, Confidas, a Cititrust affiliate located in Switzerland, acted as Trocasa's manager and handled all administrative requirements. Trocasa opened two private banking accounts, one with Citi in London and another with Citi in Switzerland. Whilst no formal documentation identifying the beneficial owner existed in London, those dealing with the account were aware of the Salinas connection to Trocasa. In Switzerland documentation did exist as

required under Swiss law identifying the beneficial owner of the funds in Trocasa as being those of Salinas. Posing as Patricia Rios and introduced to Citibank Mexico by Citibank New York, Salinas' girlfriend (Patricia Rios Castañón would only become Patricia Salinas through marriage later in 1993), she deposited peso cheques drawn on Mexican banks with Citibank Mexico, even though she had no account there. Citibank Mexico converted the pesos into US\$ and wired the funds to Citibank New York for receipt into a Citibank Concentration account. These funds were received from Citibank Mexico as being from numerous entities including "Tyler Ltd and PS." Once in the concentration account in New York the funds were then wired to London or Switzerland and invested as directed by Citibank New York to Citibank London and Switzerland. On occasion Mr Salinas did contact for example Switzerland making direct contact and making investment decisions.

The very critical view taken by the US Senate of Citibank and its dealings with Raúl Salinas contrasts with the evidence provided to the US Senate by Salinas' Client Adviser 32 year Citibank veteran Amy Elliot. It is also worth noting that US regulators confirmed that Citibank did not appear to be in violation of any US laws and or regulations then in force. Ms Elliot was born in Cuba and emigrated to the US in 1961 when she was only 17 years old, with her family being persecuted by the Castro government. Ms Elliot joined Citi in 1967 and worked in a variety of positions until 1983, when she joined the Private Bank. In 1992, whilst as the Mexico Team Leader in New York and having worked for 8 years covering Mexican clients, she became the client relationship manager for Raúl Salinas who wanted to establish a new relationship. Ms Elliot first met Raúl Salinas in early 1992, at the same time as his brother, Carlos Salinas, was the President of Mexico. At this time President Salinas was seen as a hero both in his own country and abroad for his reforming agenda, Elliot told the US Senate. Elliot further explained that in Mexico in the early 1990s, the Salinas family was known as an old, distinguished family that had wealth going back many generations.

Raúl Salinas was referred to Ms Elliot by an existing 10 year Citibank client, (the then existing Agriculture Minister in Mexico) covered for 4 years by Ms Elliott and where the existing client personally attended at the Bank in New York, together with Mr Salinas to make the introduction. The existing long standing client had been close friends with Raúl Salinas since childhood and he told Ms Elliott he had worked with Salinas on numerous business projects. According to Ms Elliot Mr Salinas requested that his accounts be structured

in the same manner as the accounts of the client who referred him to the Bank. The use of a personal investment company, or "PIC," to hold his investments, and the method of transferring monies provided for confidentiality and also allowed for efficient tax and estate planning.

Confidentiality was required because many wealthy Mexicans are frequently the targets of kidnappings and other violent crimes in Mexico. Mr Salinas initially deposited US\$2mio, money, in fact, that was being returned to him by the referring client as a result of a joint venture that did not go through. In mid-1993 Mr Salinas started to deposit larger amounts of money at Citibank. The Wealth was believed to have been generated from a number of sources. First, from the sale of his construction company and secondly as Mr Salinas was a member one of Mexico's wealthy families and the children often received their inheritances, called patrimonio, while their parents were still alive, this was a source and thirdly the Mexican stock market had been doing very well, and Ms Elliot believed that Salinas' financial investments and the patrimonio had grown considerably. Lastly Mr Salinas married Paulina Castañón in June of 1993, and she had received a substantial divorce settlement. According to Ms Elliot for these reasons, the size of the account, the structure and the activity in the account never appeared suspicious to her. In particular Mr Salinas' decision to transfer money out of Mexico and from Mexican pesos into US\$ in 1993 -- which was the year before the Mexican Presidential election -- is exactly what many other wealthy Mexicans, including other Mexican clients, were doing at the time. This is, sadly, a tradition in Mexico because of the political and economic instability that occurs in the country around Presidential elections. The value of the peso and the Mexican stock markets usually drop preceding Presidential elections. There seems to be a fear that, with political transition, Salinas could suddenly find himself under enormous political attack. So, there were large amounts of money leaving Mexico in the 1993-94 time frame, including the funds of Raúl Salinas. That, in the context of Mexican politics, was not surprising and it was certainly not illegal; rather it was prudent and happened like clockwork every Presidential election year.

Citigroup Chairman and Citibank Co Chairman, John Reed gave evidence at the Senate hearings and admitted that controls over Citibank's private banking unit, had been unsatisfactory. He said there had been "oversight lapses" in the early 1990s, but that since then the bank had taken steps to rectify this. Committee chair Senator Susan Collins, a Maine Republican, said: "Too often, Citibank's private bank essentially paid lip service to its

own procedures. She went on, "We cannot allow the integrity of our banking system to be sullied by the dirty money that fuels the engine of criminal enterprises both here and abroad," and "Our banks must be vigilant in their efforts to detect and report criminal activity and avoid acting as conduits for money laundering."

Ms Elliot concluded her testimony at the US Senate stating, "The world in which I operated as a private banker in the early nineties was different from the private banking environment today. Procedures, technology, and safeguards are very different today at Citibank. Today, given all the changes that have taken place at the Bank, there is much more I would be required to do to accept a new private banking client such as Raúl Salinas."³

In October 1998, the Federal Reserve proposed that banks develop a profile of their customers' typical transactions and monitor them for deviations.

Position: Brother to President of Mexico
When: 1998-1994 (Brothers term of Office)
Amount involved: US\$100s mio
Country: Mexico
Key date: 1995

Mobutu Sese Seko

Mobutu was president of Zaïre from 1965 to 1997. In 1960 Mobutu was appointed state secretary in the first government of President Lumumba and later becoming head of the Army. In 1965 President Lumumba was assassinated and Mobutu took over the Presidency using his Army position as his power base. Mobutu introduced a sophisticated system of power and corruption shamelessly taking much of the profits of one of the richest nations in Africa due to its abundant mineral resources. As a bulwark against communism during the cold war, Mobutu used his pro-west credentials to obtain western development aid, which he then diverted and benefited from.

Mobutu became known for his lavish standard of living. During the 1980s the official budget allocated for the President exceeded the budget for roads, schools and hospitals combined. Anecdotes for his spending include his trips in a chartered Concorde to go to his dentist in Nice – accompanied by a 747 for his luggage and entourage. Perhaps to illustrate the corruption endemic in Zaïre during the Mobutu Presidency, the following quote came from Mobutu himself, "When I need one million, I ask my private secretary. He calls the Prime Minister asking for two million. The Prime Minister asks the Finance Minister for three million who in turn calls the Governor of the Central Bank

demanding 4 million. In the end I (Mobutu) get my million." Mobutu had an important real-estate portfolio around the globe including houses and apartments in many western countries and used the state entities (central bank, embassies etc.) to settle his private bills. Mobutu's imperial behaviour whilst objectionable to many was not unusual in the context of earlier times. His exhibition of power and potency were reflections of earlier times when African Kings ruled absolutely. Eventually and after more than three decades in power, Mobutu's reign came to an end in 1997.

With Mobutu weakened with little support from the West following the ending of the Cold War and the state seen as chronically corrupt, rivals rose to oust Mobutu. One rival Laurent-Desiré Kabila who secured support from Rwandan troops was able to force out Mobutu who fled the country dying shortly thereafter of cancer. Kabila would die soon after from a heart attack but not before renaming the country The Democratic Republic of the Congo and enabling the succession of his son who remains the current President. Mobutu left the country in a much poorer state than it was before colonial times. According to Transparency International in 2004, he was the third most corrupt leader who stole US\$5bio.

Country: Zaire
Key date: 1997 (forced into exile)

Augusto Pinochet

Augusto Pinochet was a Chilean general who assumed power in a coup d'état in September 1973 becoming President until 1990 when he was finally forced to hand over to a democratically elected government. His period of power was to be marked by widespread abuse of human rights including torture and murder. The number of people believed to have been killed under his orders and by the "death squads" he formed will never be known but it has been claimed that as many as 3,000 were murdered with ten times that number being tortured and even more being imprisoned or interned for protesting against his rule. His period of power saw the junta which he led sell state controlled industries and land to the private sector a process that offered plenty of opportunity to "skim" money off for his own benefit. The desire to ensure the Chilean economy remained stable ensured that international donors and financial institutions such as the World Bank and International Monetary Fund made significant sums of money available and these policies eventually saw the economy prosper even though its levels of foreign debt soared. Following the return of a democratic government in 1990, Pinochet left the country to settle in the UK having been sworn in as a "senator for life"

and been granted immunity from prosecution.

He was however, then arrested in 1998 following an extradition request from the Spanish authorities alleging abuses of power but following a long battle in the courts was finally released without trial in March 2000 and returned home to Chile claiming that he was in poor health. In March 2000, the Chilean congress removed his immunity from prosecution and in August of that year he was finally indicted for the disappearance of 75 individuals whose bodies had never been found which made it impossible to bring a charge of murder. In 2002 these charged were dismissed on the grounds that Pinochet was suffering from senility and he then resigned from his seat as a senator.

In 2004 the Supreme Court overturned the previous decision and he was then charged with several murders and other offences which was merely the start of a set of international actions and indictments arising from long standing investigations. Pinochet, nearing his 90th birthday, was placed under house arrest. In 2006 he was charged with a further set of offences including further kidnapping and torture charges together with involvement in the production and distribution of cocaine, the proceeds of which has allegedly been transferred offshore and into accounts controlled by Pinochet.

The financial dealings of Pinochet and his associates was the primary focus of an investigation by US authorities which centred on a network of accounts and other assets held at a number of US financial institutions and Riggs Bank in particular. Partly as a result of these findings, Pinochet's wife and four of his children together with business and political associates were all charged with tax evasion along with other offences linked to the funds uncovered by the US investigation. At least US\$27mio was alleged to have been illegally obtained and transferred through a network of trust funds and shell corporations. For more information see Riggs Bank at Part 2, Section 8, Enforcement Cases below.

In 2005 "The Guardian" newspaper alleged that Pinochet had been the beneficiary of "commission" payments related to the awarding of substantial arms related contracts to the Chilean armed forces. Pinochet was never to stand trial for these offences as he suffered a heart attack and died on the morning of 3 December 2006 an event that caused widespread celebration within Chile

Country: Chile
Key date: 1998 (arrested under a Spanish Warrant)

Special Focus 3 Sani Abacha



Sani Abacha was born in Kano Nigeria on 20 September 1943 and rose through the ranks of the Nigerian military before assuming overall command of the military forces in that country when he was appointed Minister of Defence in 1990. At the same time, he pursued a parallel

career in politics and through a combination of both positions became the de facto President of Nigeria from 1993 to 1998, following the annulment of elections, from which major unrest ensued. Whilst continuing to publicly assert his commitment to bringing democracy to Nigeria he pursued a campaign of repression aimed at undermining and, in some cases, eliminating opposition action which was criticised by human rights campaigners, civil rights lawyers and other pressure groups and commentators around the world. Abacha's response to this was to ban political activity and exert control over all forms of the Nigerian press as well as surrounding himself with a loyal military powerbase which secured his position.

His ability to do so was assisted by the increasing value of Nigeria's reserves of oil which generated considerable income and opportunities for him, members of his family and close colleagues to siphon off huge amounts of money and deposit it in accounts held around the world. Frequently this was done through corruption associated with the tendering and subsequent award of contracts awarded to foreign entities and individuals operating in the petro-chemical industry sector.

According to post-Abacha government sources, between US\$3-4bio or up to 10% of all Nigeria's oil revenues during the five years he was in power was illegally diverted and moved offshore. The schemes to steal and subsequently launder the money varied. In one scheme, Abacha's National Security Advisor would simply make a letter request for funds for unspecified "security needs." Abacha would countersign his approval on the letter, and his national security advisor would present the letter for payment to the Nigerian Central bank. Money was issued in traveller's cheques in blank (the first embezzlement of this type involved US\$2mio in Thomas Cook traveller's cheques being issued in a single day), cash, and wire transfers. Cash was deposited into Nigerian accounts of local business, smuggled overseas and deposited into foreign institutions, and wire transfers were deposited into accounts in false names, shell and bearer share companies, and trusts.

Another scheme involved an overbilling and kickback scheme, in which a corrupt company would supply goods to the government at grossly inflated prices and then kick back a portion to Abacha and his cronies. In one instance, the government of Nigeria paid US\$110mio for vaccines that were in fact worth less than US\$23mio. In another instance, he directed Ismaila Gwarzo, his National Security Advisor, to present him with false funding requests for security operations or equipment, which he had the power to authorise, and would do so. These funds would then be remitted to Gwarzo in cash (US\$1.31mio and £413mio) or in travellers cheques from the Central Bank of Nigeria. The funds would then be taken directly to Abacha's house.

Abacha died in June 1998 while at the presidential villa in Abuja. He was buried on the same day, according to Muslim tradition, without an autopsy. This fuelled speculation that foul-play was involved and that he may have been poisoned by political rivals via prostitutes. Whilst Nigerian military rulers cited his cause of death as a sudden heart attack it is suspected that he was in the company of six teenage Indian prostitutes imported from Dubai. It is thought that these prostitutes laced his drink with a poisonous substance, making Abacha feel unwell around 4:30am. He retired to his bed and was dead by 6:15am.

Following his death, recovery of the looted assets became a major objective for subsequent Nigerian governments with requests for mutual legal assistance being submitted to Liechtenstein, Luxembourg, Switzerland, the UK, Jersey and the US. Assets of approximately US\$2.6bio have been identified, with half of this being frozen and returned to Nigeria, following major legal battles. The remainder remains subject to dispute. As the assets were being identified, it became clear that major financial institutions and by extension major financial centres had failed to establish money laundering controls sufficient to counter the systematic looting of state assets on such a grand scale. The sheer size of the assets involved and the numbers of financial institutions involved across all the major financial centres directly led to a re-evaluation and a recognition that controls needed to be enhanced and in particular expectations rose dramatically as to how a financial institution should treat prospective business relationships with politicians and their direct family and associates. In future, relationships with individuals identified as PEPs or with entities with a significant PEP involvement in their management would need to be subject to significant additional scrutiny. According to Transparency International in 2004, he was the fourth most corrupt leader who stole US\$2.5bio.

Position: President of Nigeria

When: 1993-1998

Amounts Involved: US\$2.5bio

Country: Nigeria

Key date: 1998 (died in office)

Pavel Lazarenko

Pavlo Lazarenko was the seventh Prime Minister of Ukraine from 1996 to 1997, promoted from his position as Energy Minister by then Ukrainian President Leonid Kuchma but soon after quickly dismissed. While in office, he exercised control over a large swathe of the economy and influenced the privatisation of Ukraine's vast natural gas sector.

During his time in government, Lazarenko engaged in many different corruption schemes including extorting funds from businesses that wished to do business in Ukraine. Shortly after leaving office, Ukrainian prosecutors began an investigation into Lazarenko's alleged corruption and the members of the Ukrainian parliament sought to lift his immunity from prosecution.

In December 1998, he was arrested by Swiss police after attempting to cross the border by car from France on a Panamanian passport. The Swiss had already started their own investigation into his financial affairs and whilst he maintained assets found in his accounts in Switzerland were legitimately earned, the Swiss court found otherwise. He was given an 18-month suspended sentence and US\$6.5mio was confiscated from his Swiss accounts. Lazarenko was found guilty in absentia as he had left Switzerland soon after his arrest after posting a US\$2.5mio bail bond. Fearful of Ukrainian prosecutors, or others from the Ukraine, claiming he had received death threats, he travelled to the US seeking political asylum. He was granted a long stay in the US though that would not be at the 18-acre estate in San Francisco, for which he is said to have paid US\$6.7mio in cash. US prosecutors accused Lazarenko of laundering US\$114mio stolen while in office in Ukraine in American banks and he remains in a US prison having been found guilty of money laundering, wire fraud and extortion.

Lazarenko used corporate vehicles to avoid direct connections between themselves and the funds, for example, in the purchase of the US property, as funds flowed from a corporate shell account (Dugsbery) in the US, which in turn had received the funds from a corporate shell account (Lady Lake) in the Bahamas, which itself had been funded by a corporate shell account in Switzerland (CARPO-53). To give a sense of the scope and the ease in which corporate vehicles were used to transfer money, Lazarenko in one instance transferred US\$78mio through the issuance of two sequentially numbered cheques, made payable to "bearer" from a US-based account in the name of a corporation and those cheques were then deposited into the accounts of two different corporations at a bank in Antigua. According to Transparency International, he is the eighth most corrupt leader who stole funds of around US\$114-200mio.

Country: Ukraine

Key date: 1998 (arrested by Swiss Police)

Slobodan Milosevic

Slobodan Milosevic was the President of Serbia from 1989 to 1997 and President of the Federal Republic of Yugoslavia from 1997 to 2000. His Presidency was marked by the breakup of Yugoslavia and the subsequent Yugoslav Wars. In the midst of the 1999 NATO bombing of Yugoslavia, Milosevic was charged with war crimes and crimes against humanity in connection with the wars in Bosnia, Croatia and Kosovo by the International Criminal Tribunal for the former Yugoslavia (ICTY) and would become known as the Butcher of the Balkans. He died in his cell at the Hague in 2006.

When UN sanctions were imposed on Yugoslavia in May 1992 because of the Bosnian war, Milosevic had already anticipated the embargo and established the infrastructure for exploiting the international banking and trading systems to bust sanctions and keep importing vital commodities. The scale of the asset transfers out of Serbia was material. According to Transparency International, Regime insiders, including Milosevic's close relatives, are believed to have taken and moved hundreds of millions of dollars abroad in private, numbered or alias accounts in Cyprus, Switzerland, Lebanon, Russia, Greece, and Israel. Whether the money was fully intended to avoid economic sanctions or also for personal use is unclear, though what's more likely is that the idea was formed for the former but later became available to those holding the assets. The monies most likely came from flawed privatisations, from siphoning off customs receipts, preferential loans to crony companies and individuals plus windfalls from manipulating the foreign exchange black market.

It is believed that Milosevic's brother, wife and daughter had bank accounts, which were later frozen, in Switzerland, according to Yugoslav government sources and western diplomats in Belgrade. Mirko Marjanovic, the former Serbian prime minister who controlled the lucrative grain export business to Russia throughout the 1990s and Dragan Tomic, a Milosevic aide and former parliament speaker also had accounts that would be frozen. Assets of approximately US\$100mio were frozen by the Swiss. Two key Milosevic supporters, Nikola Sainovic, a former deputy prime minister who controlled the precious metals trade and who was also indicted for war crimes in Kosovo, and Dusan Matkovic, ex-deputy leader of Milosevic's Socialist party and head of the giant Sartid steel works at Smederevo outside Belgrade, had bank accounts in Beirut, according to a former banker inside the regime. The banker masterminding the financial system was Borka Vucic a Milosevic family friend. Before returning to head Serbia's biggest bank, Beogradsko Banka, in 1998, she spent nine years in Cyprus as head of the bank's offshore subsidiary. The operation was centred on Cyprus because of its banking secrecy, offshore companies culture, and the sympathy of Greek Cypriots for the plight of their fellow Orthodox Serbs. Cyprus was the conduit for billions of dollars in cash from

Serbia. The funds were then dispersed globally or into the accounts of scores of anonymously owned offshore companies registered in Cyprus. In the early 1980s, Milosevic was President of Beogradsko Banka and Mrs Vucic was his deputy. If there is no doubt that Mrs Vucic was the linchpin of the Milosevic money system, she vehemently denies handling Milosevic family money or doing anything illegal. She insists she was only doing her patriotic duty in helping her country to evade sanctions. "I know Mr Milosevic quite well and I know the family. He was a fighter, a good banker and a good President," she said "But we had no business at all with the family. I believe they have some other banks but not Beogradsko." All through the 1990s she headed Beogradsko Banka's offshore subsidiary in Cyprus, the biggest offshore bank on the island, handling the accounts of the myriad Serbian offshore companies established there, such as Yugometall, the state company trading in metals. According to Transparency International in 2004, he was the fifth most corrupt leader who stole US\$1bio.

Country: Former Yugoslavia

Key date: 1999 (charged with war crimes)

Alberto Fujimori

Alberto Fujimori, the son of Japanese immigrants, became the president of Peru between 1990-2000. When Fujimori took office, the country's economy was in a state of collapse. Even worse, Peru was in the midst of a war and seemed destined to fall into the hands of the Sendero Luminoso or the Shining Path and the Túpac Amaru or the MRTA terrorist movements which controlled about a third of the country. Abimael Guzmán, a philosophy lecturer in the University of San Cristóbal de Huamanga, in Ayacucho, founded the Shining Path in 1970 as a Maoist breakaway movement from the pro-Russian Peruvian Communist Party. Poverty and injustice made Ayacucho a fertile breeding ground for the movement which started a campaign of armed insurrection in 1980. By the middle of the decade several thousand guerrillas were operating in rural areas and by the late 80s urban terrorism was also a real problem. The Movimiento Revolucionario Túpac Amaru, generally known by its initials, MRTA, or as Túpac Amaru named after the last Inca ruler who was assassinated by the Spaniards in 1572 was smaller and less extreme than Sendero Luminoso, and started its guerrilla campaign in 1984. Alberto Fujimori eventually with assistance from his security chief Vladimiro Montesinos and the army defeated the terrorists, pivotal to which was the capture of Guzman. The war against terrorism is estimated to have cost 30,000 lives. Fujimori's popularity soared but there were influential Peruvians who were troubled by his autocratic rule. After the Sendero Luminoso's grip on rural areas was weakened the Peruvian government began to tackle the drug dealers with some success. Nevertheless the revelations that the Peruvian intelligence services, headed by Mr Montesinos had been caught on TV bribing parliamentarians led to further revelations

including that at one stage drug traffickers paid protection money to the government, tarnished the government's record and was so scandalous that it also brought down Fujimori. On 17 November 2000 Alberto Fujimori arrived unexpectedly in Japan after attending a summit of Asia-Pacific leaders in Brunei. Three days later he faxed his resignation to Congress and claimed exile status in Japan from where extradition was not possible. In November 2005 Fujimori sought to achieve his goal of returning to power and flew to Chile to begin his campaign, only to be arrested by the Chilean authorities. Eventually he would be extradited to Peru and on 11 December 2007 he received his first conviction and was sentenced to six years in prison for abuse of power later being also sentenced to serve 25 years in prison for further crimes. According to Transparency International in 2004, he was the seventh most corrupt leader who stole US\$600mio.

Country: Peru
Key date: 2000 (resigned as Peru's President due to corruption scandal)

Vladimiro Montesinos

In August 2000 President Fujimori held a news conference to announce the interception of a large consignment of arms from Jordan destined for FARC guerrillas in Colombia and he gave the credit for smashing the operation to his right hand man, Vladimiro Montesinos. However, the Jordanian government claimed that it had sold the arms to the Peruvian armed forces. Not long afterwards, on Thursday 14 September 2000 a video was broadcast that was to lead to the fall from power of Alberto Fujimori and to the arrest and imprisonment of Montesinos. The video, that had fallen into the hands of one of the opposition parties in Peru, showed Montesinos, giving a bribe of US\$15,000 to congressman Luis Alberto Kouri to switch sides in order to try and ensure that the government's favoured candidate would be chosen as the President of Congress. According to one later report Montesinos himself had been responsible for the arms sale to FARC, angering the CIA, who turned against a man with whom they had previously had close links, and a group of Peruvian army officers who were emboldened to break into his office and steal the tape - one of a collection of thousands incriminating politicians, officials and military officers.

Whatever the truth about the origin of the video, in the uproar that ensued following its broadcast, Fujimori announced that he would hold new presidential and parliamentary elections in which he himself would not be a candidate. At the same time, he announced the dissolution of SIN, el Servicio de Inteligencia Nacional (the National Intelligence Service), of which Montesinos was the de facto chief. The parents of the

spy chief, regarded by many as Fujimori's Rasputin, were communists and therefore they named their son, who was born in Arequipa in 1946, Vladimir Ilyich after Lenin, an ironic choice for the boy who was to grow up to become the pillar of a right-wing regime. By coincidence Arequipa was also the birthplace of the novelist Mario Vargas Llosa, Fujimori's opponent in the 1990 election, and Shining Path leader Abimael Guzmán. In 1966 Vladimiro Montesinos joined the army and subsequently became the personal adjutant of another officer from Arequipa, General Mercado Jarrín. When the President, General, Juan Velasco Alvarado made Jarrín his prime minister in January 1973, Montesinos moved closer to the reigns of power in what was a left-wing regime. Soon it became apparent that information was being leaked to the US embassy and suspicion fell on Montesinos. When General Guillermo Arbulú took over as commander-in-chief of the army in 1976, Montesinos was transferred to a remote garrison of El Algarrobo near the Ecuador border. Montesinos stayed there only a matter of days before flying to Washington where he had meetings with officials in the CIA but on his return to Peru he was arrested and convicted of falsehood and desertion of command, expelled from the army, and sentenced to a year's imprisonment. While in prison he studied law and on his release specialised in defending people accused of tax fraud and drug trafficking. As the cocaine barons had corrupt allies in the army and police the information Montesinos acquired through his job made him an increasingly powerful figure. When General José Valdivia was accused of having been responsible for the massacre of innocent civilians in the Shining Path stronghold of Ayacucho in 1988, he turned to Montesinos for help and the case against him was dropped. Even SIN found Montesinos useful because of his contacts and files on all sorts of people and he began to supply the agency with information.

When, during his campaign for the Presidency in 1990, Fujimori was worried about accusations of tax evasion which were damaging to a candidate who made much of his clean reputation, General Díaz, the boss of SIN, suggested that Montesinos should help him. From then onwards Fujimori found himself increasingly dependent on Montesinos whose reputation became even more controversial. Demetrio Chavez also known as "El Vaticano" at his trial in 1996 claimed that he had paid US\$50,000 a month to Montesinos for protection, but when he reappeared in court about a week later, apparently somewhat the worse for wear, he withdrew the accusation saying that he had been "confused" when he made it. The money mentioned in El Vaticano's recanted statement was relatively trivial compared with the amounts mentioned in allegations

after Montesinos fell from power. Roberto Escobar, the brother of the former head of the notorious Medellin drug cartel in Colombia, Pablo Escobar, who was killed in 1993, wrote a book published in January 2001 called *Mi Hermano Pablo* (My Brother Pablo) in which he claimed that Fujimori's first election campaign was financed by a donation of US\$1mio of drug money and that total payments to Montesinos to ensure that Escobar's planes carrying partly processed cocaine were not shot down in Peruvian airspace, came to US\$45mio.

After the broadcast in September 2000 of the video showing him bribing a congressman, Montesinos left for Panama but, after being refused asylum in that country, returned to Peru and immediately went into hiding. President Fujimori gave orders for the arrest of his former spy chief but his own hold on power was almost at an end. On 2 November Switzerland announced that it was freezing about US\$50mio in five bank accounts linked to Peru's ex-spy chief, prompting the Peruvian government to launch a probe into allegations that Montesinos laundered money through Swiss banks. Evidence of other unexplained bank accounts (in various places, including the Cayman Islands, Uruguay and New York) containing US\$274mio allegedly amassed from arms deals and drug trafficking was soon uncovered. Even those discoveries leave the bulk of the US\$800mio thought to have been taken illegally from the Peruvian government's coffers, unaccounted for. On Saturday, 23 June 2001, Vladimiro Montesinos was arrested in Venezuela, a month after Jose Guevara - a former Venezuelan intelligence service agent, had attempted to withdraw part of the US\$38mio Montesinos held in a frozen account at a bank in Miami. Guevara opted to reveal the fugitive's whereabouts in return for the US\$5mio reward offered by the Peruvian government. Ketin Vidal, Peru's interior minister, flew to Venezuela to arrange the handing over of the former SIN boss. Almost a year later, on 3 May 2002, it was reported that the Peruvian government had still not paid the promised US\$5mio reward for the capture of Montesinos and was trying to decide between the competing claims of a banker, a bodyguard and a private investigator. On 1 July 2002 Vladimiro Montesinos was convicted of illegally controlling Peru's spy agency and he was sentenced to nine years and four months in prison. Nearly a year later, on 29 May 2003 he was sentenced to eight years imprisonment on embezzlement charges. Altogether Montesinos faces about 70 different trials. The legal procedures against him are still not complete and in April 2005 he was sentenced to five years imprisonment after he pleaded guilty to accepting US\$15mio in "severance pay" from President Fujimori as their regime collapsed.

Country: Peru
Key date: 2000 (film broadcasted showing bribe paying PEPs)

Mohamed Suharto

Mohamed Suharto was the second President of Indonesia holding office from 1967 to 1998, resigning that year after huge protests by Indonesians. He held office for about 31 years and was sometimes popularly referred to in the media as Pak Harto, or Father Harto and 'The Smiling General'. Suharto and his family used their power to enrich themselves and their friends, gaining billions of dollars through their control of government enterprises and charities and their acceptance of kickbacks for state contracts. Ties to Suharto were seen as an essential prerequisite to doing business in Indonesia, with those in favour being given lucrative government contracts often at the expense of economic efficiency. Suharto's cronies used their positions for personal enrichment and to enhance their political power. His six children wielded significant influence and launched many questionable business ventures, funded from established government foundations. Suharto's wife came to be known as 'Madam Ten Percent' due to the commission she demanded from business deals where her support was solicited.

The collapse of Indonesia's economy following the crony capitalism of the Suharto Regime was inevitable but was triggered by the Asian financial and economic crises in late 1996. This led to popular discontent with Suharto's rule and provoked widespread rioting forcing his resignation in 1998. A World Bank report that year estimates that at least 20-30% of Indonesia's development budget over the previous two decades had been embezzled for personal and political gains. The report went on to state that "Indonesia is in deep economic crisis." "A country that achieved decades of rapid growth, stability and poverty reduction is now near economic collapse," a study by the bank found. "No country in recent history, let alone one the size of Indonesia, has ever suffered such a dramatic reversal of fortune."

In 1998, according to Time magazine, the Suharto family fortune was worth an estimated US\$15bio in cash, shares, corporate assets, real estate, jewellery and fine art. US\$9bio of this was reported to have been deposited in an Austrian bank. The family was said to control about 3.6 million hectares of real estate in Indonesia, including 100,000 square metres of prime office space in Jakarta and nearly 40% of the land in East Timor. Over US\$73bio was alleged to have passed through the family's hands to friends and family

during Suharto's 32-year rule. By 2000 Suharto came under investigation for the corruption that occurred during his Presidency, being first placed under house arrest and then charged with embezzling US\$571mio of government donations to one of a number of foundations under his control and then using the money to finance family investments, though a panel of court-appointed doctors found him permanently physically and mentally unfit to stand trial. Indonesian prosecutors again tried in 2000 bringing a US\$1.5bio civil lawsuit against Suharto to recover funds allegedly siphoned from the Supersemar educational foundation set up in 1974. The prosecutors alleged that, beginning in 1978 and continuing until Suharto's ouster, 85% of the money sent to the foundation was embezzled. The court ordered Supersemar to pay the government US\$110mio in compensation but failed to find Suharto responsible. Whilst Suharto escaped justice his youngest son, Hutomo (Tommy) Mandala Putra, was found guilty and jailed for 15 years for organising the murder of a judge who in September 2000 sentenced him to 18 months for his role in a land deal, however he was released on parole in 2006 serving less than five years of the original 15 year sentence. According to Transparency International, Mohammed Suharto was the number one most corrupt leader who stole funds of around US\$15-35bio. No funds were ever recovered abroad and returned to Indonesia.

Country: Indonesia
Key date: 2000 (Under investigation for corruption)

Joseph Estrada
Joseph "Erap" Ejercito Estrada was the 13th President of the Philippines from 1998 to 2001. He is the only Filipino president to have resigned from office. Before joining politics, he was a popular film actor who played a lead role in over 100 films and won awards for his performances. Estrada's tenure as president was short-lived, however, as a corruption scandal erupted in October 2000 when a fellow politician claimed that Estrada had accepted millions of dollars worth of bribes. In November the Philippine Senate began an impeachment trial, but it was abandoned after some senators blocked the admission of evidence. On 20 January 2001, Estrada was ousted amid mass protests, and his Vice President, Gloria Macapagal Arroyo, ascended to the Presidency. Later that year Estrada was brought to trial on charges of large scale corruption and accused of having procured more than US\$80mio through bribes and corrupt dealings. Estrada denied the accusations, calling them politically motivated, and he remained relatively popular in the Philippines despite the charges. In September 2007 he was convicted and sentenced to a maximum of 40 years in prison. The

following month, however, Estrada was pardoned by then President Arroyo. According to Transparency International who published a list in 2004, he was the tenth most corrupt leader who stole funds of around US\$78-80mio

Country: Philippines
Key date: 2001 (ousted as Philippine President due to corruption scandal)

Paulo Maluf

Paulo Maluf is a successful Brazilian politician with a career spanning over four decades having been State Governor of São Paulo, Mayor of the City of São Paulo, Congressman and Presidential candidate. As of 2011, Maluf is on a second consecutive term as a Federal Deputy. His political base is on the right-wing in the Progressive Party of Brazil. His career has been plagued with substantial allegations of corruption. He was convicted on one charge in 2001 by the Brazilian courts, and is currently wanted for fraud conspiracy and theft by Interpol.

Paulo Salim Maluf, the son of Lebanese Christian immigrants grew up in São Paulo, and in his youth he was a self-acknowledged playboy with a taste for fast-racing sports cars. Maluf entered professional politics thanks to his family's friendship with the then military President Artur da Costa e Silva, with whom he shared a common interest in horse racing and gambling. Based on this friendship, he was appointed mayor of São Paulo in 1969. An early act was to suspend the construction of the São Paulo Metro and build instead one of the most controversial constructions in Brazil: the Costa e Silva elevated expressway, also known as Minhocão ("Big Earthworm" in Portuguese). In 1972, following his mayoralship, he served as secretary of transport of the state of São Paulo and then afterwards elected governor for the state of São Paulo in 1978. During his ensuing term (1979–1983), Maluf spent wildly on public works, including some schemes of doubtful validity, such as on a failed plan to move the state's capital city. It was because of such schemes that one of the most notable accusations of corruption against him emerged, concerning the oil company Paulipetro. This was a state company founded by Maluf during his tenure as governor with the purpose of digging the state for oil and which consumed around US\$500mio whilst drilling 21 holes and finding nothing but a few pockets of natural gas and water. By then, Maluf had already fostered a reputation "for engaging in corrupt machine politics". Maluf was a presidential candidate in the first direct presidential elections in 1985, though he didn't do well. Maluf was still able to forge a successful career in post-dictatorship Brazil, despite his perennial reputation for corruption. One notable example of the allegations of corruption that surfaced around Maluf was the Ayrton Senna tunnel, which passes underneath Ibirapuera Park and cost more, per kilometer, than the UK/French Channel Tunnel with allegations that the tunnel cost

over US\$400mio more than it should.

Under dispute is Maluf's personal wealth, which critics attribute to his involvement in corruption scandals; supporters, conversely, point to a legitimate origin of such wealth in his family's companies. Maluf has been convicted of corruption multiple times, but only in 2001 was the sentence considered final, with no possibility of appeal. At the time, he was forced to pay approximately R\$500,000 to the state. Many of his alleged crimes cannot be prosecuted, due to the nature of the Brazilian statute of limitations. In early September 2005, Paulo Maluf and his son Flávio Maluf were temporarily arrested by the Brazilian Federal police, under the charge of intimidating witnesses of an ongoing investigation. They were only incarcerated for a few weeks. So notorious is Maluf's reputation that in Brazil the verb malufar was created, meaning "to steal public money".

In the 2006 elections, Maluf ran for a seat in the Brazilian Chamber of Deputies, being elected as the candidate for the federal legislature with the greatest number of ballots cast personally for him. In 2007, Robert M. Morgenthau of the Manhattan's District Attorney's office issued an indictment against Paulo Maluf for Money Laundering in relation to kickback and inflated invoice scheme that allegedly stole US\$11.6mio from a Brazilian road contract project totalling US\$140mio. In March 2010, Paulo and Flávio Maluf were included in an Interpol Red notice, however this arrest warrant is not valid in Brazil because the Brazilian Constitution does not allow for the extradition of Brazilian citizens.

Country: Brazil
Key date: 2001 (convicted of corruption in Brazil)

Arnoldo Alemán

Arnoldo Alemán was born in Managua and rose to become the President of Nicaragua in 1996. In 1979 following a short-lived civil war, the Marxist Sandinista guerrillas came to power. The US sponsored anti-Sandinista Contra guerrillas through much of the 1980s. In 1996 he campaigned for President under a strong anti-Sandinista platform. It is reported that unidentified individuals attempted to shoot Alemán, killing one of his bodyguards in the process. He defeated Daniel Ortega, the Sandinista leader, by 48% of the vote to Ortega's 40%. Many claimed widespread election fraud and Ortega refused to concede.

Alemán was successful in promoting economic recovery with reduced inflation and growth of GDP. Foreign investment grew during his administration, which helped to improve Nicaragua's infrastructure. Alemán was constitutionally barred from running for another term, and was succeeded by his vice president, Enrique Bolaños who soon raised serious allegations that Alemán had engaged in massive corruption during his administration for example, one scheme was reported to have involved several members of Arnoldo Alemán's closest family, including a brother and sister,

as well as Alemán's daughter María Dolores Alemán, and her husband Jerónimo Gadea. Ex-ministers and close friends were also charged, some of whom fled the country. However, one of the central figures in the corruption plot, the former Chief of Department of Taxes Byron Jeréz, was imprisoned on the basis of another charge of corruption. Several foreign governments froze Alemán's bank accounts in their countries and threatened to confiscate the funds. In such cases, his defence has been to claim that the funds were not stolen, but that they came from his coffee plantations.

Alemán was formally charged in 2002, and in 2003 he was sentenced to a 20-year prison term for a string of crimes including money laundering, embezzlement and corruption. During his trial, prosecutors produced evidence showing that he and his wife had made extremely large charges to government credit cards, "including a US\$13,755 bill for the Ritz Carlton hotel in Bali and US\$68,506 for hotel expenses and handicrafts in India." Because of health problems, he was allowed to serve his prison term under house arrest. He was also barred from entering the US. In 2009, Nicaragua's Supreme Court overturned the 20-year corruption sentence against Alemán. The decision generated much controversy. Many believed that Alemán struck a secret deal with now President Ortega and leader of the Sandinista Party, who wielded considerable influence and control over the courts, in exchange for persuading many of the now opposition to co-operate with Ortega. According to Transparency International in 2004, he was the ninth most corrupt leader who stole US\$100mio.

Country: Nicaragua
Key date: 2002 (corruption charges laid)

Frederick Chiluba

In the late 1990s and early 2000s, then-President of Zambia, Frederick Chiluba, together with the Head of the Zambian Security Intelligence Services, Xavier Franklin Chungu, concocted a scheme to embezzle over US\$70mio from the Zambian Treasury. In one aspect of the scheme, Chiluba and Chungu, through an intermediary, appeared to contract with a Bulgarian company for the purchase of military equipment, including helicopters, aircraft and weapons. US\$20mio, in a number of tranches, was paid by the Zambian Treasury to two accounts in Belgium and Switzerland to satisfy the contract. In reality, no arms were ever delivered and the money that had been transferred into the accounts was dissipated by Chiluba, Chungu and their associates. The withdrawals from the accounts, purportedly set up to purchase arms from Bulgaria, included US\$7.6mio being withdrawn in cash. Some cash withdrawals were quite large, including one US\$1.3mio withdrawal. Other transfers were to law firms associated with the Zambian President and his associates.

Country: Zambia
Key date: 2003 (corruption charges laid; acquitted (in Zambia) 2009)

Saddam Hussein

Saddam Hussein Abd al-Majid al-Tikriti was the fifth President of Iraq, rising to ultimate power in 1979, long a leading member of the revolutionary Arab Socialist Ba'ath Party, which espoused ba'athism, a mix of Arab nationalism and Arab socialism. Saddam played a key role in the 1968 coup and later Vice President and then President before being captured and executed following the 2003 Iraqi invasion by Western forces. Saddam was credited with the creation of internal security forces through which he tightly controlled conflict between the government and the armed forces.

In the early 1970s, Saddam nationalised oil and other industries. The state-owned banks were put under his control, leaving the system eventually insolvent mostly due to the Iran-Iraq War, the Persian Gulf War, and UN sanctions. Following his capture in December 2003, the trial of Saddam took place under the Iraqi interim government. On 5 November 2006, Saddam was convicted of charges related to the 1982 killing of 148 Iraqi Shi'ites and was sentenced to death by hanging. He was certainly responsible for many more atrocities than these and during his time in office Saddam was widely condemned for the brutality and corrupt nature of his dictatorship. His execution was carried out on 30 December 2006.

The UN sanctions placed upon Iraq for its invasion of Kuwait were relaxed because of the hardships suffered by ordinary Iraqis, with a formal agreement being agreed between Iraq and the UN in 1996 with the coming into being of the Oil-for-Food Programme, ('Programme'), which was systematically manipulated by Saddam. Under the Programme, which ended in 2003 with the invasion of Iraq by the US and its allies, Iraq would be permitted selective sales of its oil with the proceeds to be deposited in a bank account controlled by the UN. The UN would use the approved purchases negotiated by Iraq and disburse payments to vendors to buy food and other goods: Iraq would be allowed to sell oil and goods prices independently and to enter into contracts directly with buyers and sellers of its own choosing. Coupled with what turned out to be lax oversight by UN Programme management, internal and external auditors, and investigatory bodies, the ability to set prices and select contracting parties ended up giving Saddam Hussein an opportunity to circumvent the Programme's purpose and realize a direct gain in the form of bribes. An investigation of the Programme was set up by the UN to determine whether charges of corruption were founded in fact. The Independent Inquiry Committee ('IIC') was chaired by Paul Volcker who was joined by Judge Richard Goldstone and Professor Mark Pieth. The report of the Committee's findings was published in October 2005. The key findings were that: the Iraqi government systematically levied bribes on oil

and goods under the Programme and the Independent Inquiry unearthed documents showing that the oil ministry and other government departments were directed to impose and collect fees on the total price of each contract, preferably prior to shipment. The illicit payments were usually a matter of cents per barrel on oil contracts and 10% of contract price for the purchase of goods. The investigators were able to locate ledgers, databases, spreadsheets and documents that tracked on a contract by contract basis the price agreed for the goods, the contract price which included the 10% uplift, and the bribe levied and collected. Many kept side letters in which the vendor promised to pay the 10%, often referred to as an 'after service sales fees'. Records were also found which showed hard currency side payments for inland transportation, in direct contravention of UN rules and agreements. This evidence was corroborated by ample evidence found in banking, embassy, and company records that bribes had in fact been paid. Embassy records in Moscow, for example, showed tens of millions of dollars transported in cash from Russia to Baghdad in diplomatic pouches, corresponding to the records kept by the Iraqi oil marketing company of bribes levied and paid on particular oil deals. In terms of humanitarian aid contracts, shippers kept proof that the suppliers for whom they were transporting goods had paid the 10% bribes. This became necessary for shippers in order to avoid Iraqi port agents refusing to unload the ship's entire cargo if any portion of the shipment had unpaid bribes. Further transportation agents who served as the primary collectors of the bribes payments had chronicled inland transportation fees paid by company and contract number. Companies and traders involved in buying the oil or supplying humanitarian aid also had maintained copious records including evidence of side payments, while banks from around the world had left a paperwork trail replete with letters of credit, deposits and money transfers. As a result of the forensic techniques employed by the skilled investigators working for the IIC, an organised web of bribes maintained by Saddam Hussein's government was discovered. Oil surcharges were paid in connection with the contracts of 139 companies, and humanitarian kickbacks were paid in connection with the contracts of 2,253 companies. The total amount of illicit income was estimated at US\$1.8bio by the IIC although subsequent analyses have put the figure much higher. The way the bribes were structured meant that they did not represent losses for the companies paying them. Instead they were, in effect, paid by the Iraqi people. They were embedded in prices: prices that were either lower than market, in the case of oil sales, or higher than market, in the case of goods. The identification of the bribes, in other words, may also represent the identification of the amounts recoverable from vendors. The models developed by the investigators and applied to the data they had uncovered indicated that Iraq routinely undervalued its oil and overpaid for humanitarian goods, even beyond the cost of the bribes. When it came to the former, it was found that once the oil surcharge scheme got underway in 1999, Iraqi oil was consistently priced under market by

an amount much greater than what was warranted by the surcharge alone. The conclusion was drawn that it was likely that the Iraqi officials wanted a wide enough margin to assure that there would be sufficient funds for the purchaser to: pocket enough profit to keep them and their partners in the schemes buying; pay the bribes; and pay various non-contractual beneficiaries, such as political parties or individuals. Since the IIC published its report, there has been a steady trickle of cases being brought against the companies involved in bribery.

Many corporates were involved and named and shamed including for example, American oil giant Chevron Corp, which agreed to pay US\$30mio to resolve US criminal and civil liabilities as well as the Australian Wheat Board where the Australian government concluded its judicial investigation in 2006 in which it was found that AWB paid more than US\$220mio in kickbacks to Saddam Hussein's regime for wheat sales and Mercedes Benz parent Daimler AG who pleaded guilty to US bribery charges and fined US\$185mio in 2010.

Country: Iraq

Key date: 2003 (Saddam captured after invasion and put on trial, later executed)

Ali Zardari - Bhutto

Mr Asif Ali Zardari is the former President of Pakistan and the co-chairman of the Pakistan Peoples Party. He was married to former prime minister Benazir Bhutto until her death in a terrorist attack in 2007. During the times his wife was prime minister (1988-90 and 1993-1996) he became known as "Mr 10%" because of his alleged role in obtaining kickbacks as an intermediary in government deals. French arms deals during the first tenure of Ms Bhutto probably are the most famous of all alleged corruption deals of Mr 10%. According to an investigative report, Zardari offered exclusive rights to Dassault to replace the fighter jets of the air Force for a commission of 5% to be paid to a Swiss corporation under his control.

Links to the Karachi bombing of 2002 where 11 French citizens were among the 15 killed are being made alleging that the bombing may have coincided with France stopping the commission payments. 19 corruption cases were filed against Mr Zardari and his wife between 1990 and 1992 alone. It is worth noting that at the time of the commission agreement, bribing foreign official was not a criminal offence in France: it was a tax deductible. In 1997 the Swiss Authorities froze more than US\$13mio assets of the Zardari and Bhutto families and handed over documents relating to corruption allegations to the Pakistani government in 1998. In 2003 the Swiss court found Zardari and Bhutto guilty of money laundering and ordered them to pay US\$11mio to Pakistan. The assets had been a commission payment by a Swiss firm. Bhutto and Zardari appealed the 2003 Swiss conviction, which required the reopening of the case in October 2007. He

was jailed for corruption between 1990 and 1993 and arrested again in 1996 in Pakistan. While in jail, he was elected to parliament (1990 National Assembly; 1997 Senate). In 2004 he was released and went into self-exile from which he returned in 2007 after the assassination of his wife. He was elected President in 2008 until 2013. Efforts to re-open the corruption cases are being pursued by the Pakistani judiciary.

Country: Pakistan

Key date: 2003 (Swiss court finding of money laundering)

Teodoro Obiang & Son ("Teodorin")

Teodoro Nguema Obiang, attained the Presidency of Equatorial Guinea, an oil rich West African State in 1979 and continues as President still today. Equatorial Guinea is one of the smallest countries in continental Africa. Obiang became President via a bloody coup d'état. Since 1979 some 12 real and perceived unsuccessful coup attempts have occurred. The 'real' coup attempts were often perpetrated in an attempt by rival elites to seize the state's economic resources, including one notable case led by Simon Mann. The discovery of sizeable petroleum reserves in recent years has made the country one of the wealthiest in the world, however, most of the country's considerable oil wealth actually lies in the hands of only a few people. Equatorial Guinea also has one of the worst human rights records in the world, consistently ranking among the "worst of the worst" in Freedom House's annual survey of political and civil rights.

According to testimony provided to the US Senate in 2004 Teodoro Obiang, banked significant sums of money offshore, at Riggs Bank in Washington where he opened multiple personal accounts for himself, for his wife and for relatives. Riggs helped establish offshore shell corporations for the President and his sons and over the course of three years, nearly US\$13mio in cash was deposited into accounts at Riggs controlled by the President and his wife. In addition, an Equatorial Guinea government account was established which received funds from largely US oil companies doing business in the country, under terms allowing withdrawals with two signatures, one from the President and the other from either his son or his nephew. More than US\$35mio from this government account was then wired to two further companies with accounts offshore, most likely owned or controlled by the President.

Teodoro Nguema Obiang Mangue (commonly referred to as Teodorin") is currently the Minister of Forestry and Agriculture in the Equatorial Guinea and is the son of President Teodoro Nguema Obiang. He is the subject of an international arrest warrant issued by France and the subject of civil forfeiture proceedings in the US for allegedly abusing his position to profit from

corruption related to the countries oil wealth. Whilst his only obvious sign of income appears to be a government salary of US\$100,000 he has amassed a personal fortune of over US\$100mio, leading the US Senate in 2004 to name him as a “major perpetrator of corruption and finally to action by both France and the US in 2011. Teodorin appears to have been undone by the level of conspicuous consumerism he undertook flaunting his extravagant lifestyle in both Europe and the US. Assets he acquired included a US\$38.5mio Gulfstream G-V Jet, a US\$30mio house in California, US\$1.8mio worth of Michael Jackson memorabilia, a Ferrari worth more than US\$530,000, to add to his collection including 8 more Ferrari's, 7 Rolls Royces, 5 Bentleys, 4 Mercedes, 2 Lamborghinis and 2 Bugattis, an Aston Martin and a Porsche.

Country: Equatorial Guinea
Key date: 2004 (US Senate hearings alleging grand corruption)

Diepreye Alamieyeseigha

Diepreye Alamieyeseigha was elected Governor of Bayelsa State Nigeria in 1999 and re-elected in 2003. In asset declarations in 1999 and 2003, Alamieyeseigha failed to reveal, as he was required to, that he controlled numerous accounts in London with millions of pounds of deposits. In 2005, Alamieyeseigha was arrested on a flight to the UK and interviewed at a London police station. One of his London properties was searched and £1mio cash was found in numerous locked bags in a locked bedroom. During his interview he denied being involved in corruption and claimed the cash was his “strategic reserve.” An analysis of the UK-based accounts associated with Alamieyeseigha showed both cash deposits and account activity highly inconsistent with its stated purpose. For example, shortly after opening one account, there was a sharp rise in deposits from £35,000 to £1.5mio.

In 2003, Alamieyeseigha also instructed a London-based fiduciary/trust company and service provider to register a company in the Seychelles of which Alamieyeseigha was the sole shareholder and director. This company then opened an account with a UK bank. The bank had predicted a turnover of £250,000, but in the first 14 months the account received deposits totalling approximately £2.7mio and, contrary to the characteristics of a functioning business, did not have any outgoings. Also, £1.6mio came from a bank in Nigeria from a contractor to Bayelsa State. Additionally, at least one of those accounts received cash deposits, often in increments of £10,000 to £15,000.

Country: Nigeria
Key date: 2005 (corruption charges laid)

Special Focus 4

Randy “Duke” Cunningham



Randy Cunningham is a US Navy veteran and was a member of the US House of Representatives between January 2003 and December 2005 and a former member of the powerful Appropriations Committee.

Cunningham's prior military experience allowed him to have significance in the military budget. As part of his duties, he had the ability to insert special requirements, known as “earmarks” into defence budgets, requiring that the military purchase a certain good or service. Some of these earmarks also mandated the use of “no-bid” contracts, which would circumvent the normal open bidding process, purportedly because the good or service was highly specialised or classified.

In 2005 Cunningham pleaded guilty to receiving at least US\$2.4mio in bribes and benefits from defence contractors. Cunningham accepted bribes, typically through asset transactions, in exchange for no-bid earmarks. In one instance, a defence contractor was able to receive millions in no-bid contracts by purchasing the Congressman's home from him at an inflated price so that Cunningham could purchase a more expensive house. To disguise the transaction, the contractor used a corporate vehicle to purchase Cunningham's house. The contractor paid additional money to the Congressman, disguised through cheques made payable to a corporate entity that Cunningham had previously established. Other similar bribes included the purchase of a yacht, nominally owned by a third party but in fact owned and used by Cunningham and the purchase of antiques and other furniture. Investigators in the case were aided by the fact that Cunningham was required to disclose his assets and his income. An examination of those records showed that Cunningham's net worth skyrocketed in a few short years, but that his net income had not.

Position: US Congressman
When: 2003-2005
Amounts Involved: est US\$2.4mio received in bribes
Country: US
Key date: 2005 (guilty plea)

Special Focus 5

Omar Bongo



Omar Bongo was Gabon's second President, (1936-2009) succeeding to the highest position at only the age of 31. Gabon whilst achieving its independence from France still maintained close relationships and retained close ties with French oil giant, Elf-Aquitaine, giving the

Company privileged rights to exploit Gabon's significant oil reserves in exchange for France's assistance in helping the young President retain his grip on power. France kept its military bases in the country and a contingent of paratroopers underwrote Bongo's rule. The President trusted no-one but the French and his own family. Bongo duly made his son, Ali-Ben, defence minister and his daughter, Pascaline, foreign minister and then chef de cabinet. He spent much time as he could in Paris, revelling in his friendship with a succession of French Presidents, particularly Valery Giscard d'Estaing and Jacques Chirac. The latter, together with President Sarkozy were the only Western leaders to attend Bongo's funeral in 2009. As a result of investigations conducted largely by US authorities and in particular the US Congress and as a result of the evidence arising out of the corruption trial in France of Elf-Aquitaine executives President Bongo's corrupt practices could be unearthed.

President Bongo had opened a foreign offshore account at Citibank in 1970, mostly out of New York. Most of the private bank accounts managed out of New York would later be held in the hands of Tendin Investments Ltd ('Tendin'), a Bahamian shell company set up in 1985. In 1985 President Bongo transferred about US\$52mio from his accounts in Bahrain to newly opened accounts in New York for Tendin. The total funds in the Tendin accounts fluctuated over time from anything between about US\$28mio to about US\$72mio including withdrawals of about US\$67mio. However records indicated that funds moving through the private bank account at Citibank under President Bongo's control since 1985 exceeded US\$130mio. President Bongo also had extensive bank credit relationships. Between 1989 and 1996 he obtained multiple loans collateralised by his deposits. Many of these loans were issued under a complex arrangement in which the bank allowed President Bongo's accounts in Gabon to incur multi-million dollar overdrafts. These were immediately covered by transfers from President Bongo's accounts in Paris. These were in turn covered by transfers from offshore accounts belonging to Tendin. It has been suggested that this three step process may

have been designed to avoid direct transfers from the Tendin offshore accounts into the President's accounts in Gabon, so as to minimise the chance that Gabon bank personnel would learn the name of President Bongo's private investment company. It appears that the President also had accounts in Paris and Switzerland, the details of which are not clear, but were thought to contain millions of dollars in allegedly improper payments by Elf. During the trial of the disgraced Elf executives, they admitted that they paid Omar Bongo US\$40mio a year for concession rights to his oil rich but economically impoverished country. The executives claim the millions of dollars were transferred directly into Bongo's bank accounts held by a close associate, his oil adviser, Samuel Dossou.

More suspicious transactions were identified this time by the US Permanent Subcommittee on Homeland Security and Governmental Affairs, in 2006, including US\$18mio in funds from Gabon wired to the US corporate bank accounts of a US lobbyist who then distributed the funds within the US and abroad, directed by President Bongo in connection with two projects to support his regime, buying US-made armoured cars and C-130 military cargo planes. Among the funds the lobbyist distributed was US\$9.2mio which he wire transferred to an account for President Omar Bongo in Malta. Other notable transactions included in 2007, President Bongo brought US\$1mio shrink-wrapped US\$100 bills into the US under cover of diplomatic immunity without declaring the cash to US authorities as required. This was discovered when his daughter first deposited the cash in a US safe deposit box and later into her US bank account. More recently, in 2007 a police investigation into real estate owned by Bongo and his family in France found that they had 33 properties in Paris and Nice, worth an estimated US\$190mio, finally forcing France to freeze Bongo's bank accounts held in French banks.

Position: President of Gabon
When: 1967-2009 (in office)
Amounts Involved: US\$100mio
Country: Gabon
Key date: 2006 (US Congressional Investigation)

Zine El Abidine Ben Ali

Ben Ali was the second President of the Republic of Tunisia. He ascended to the office of President on 7 November 1987. He was subsequently reelected with enormous majorities exceeding 90% every time; the final reelection was on 25 October 2009. On 14 January 2011, following a popular uprising called the Tunisian Revolution, he was forced to step down and flee the country to Saudi Arabia along with his family, ending his 23-year grip on power. Ben-Ali's government was deemed authoritarian and undemocratic by independent international human rights groups such as Amnesty International and Freedom House. They criticised Tunisian officials for not observing international standards of political rights and interfering with the

work of local human rights organisations.

Ben Ali and his family are accused of corruption, which was a major contribution to the 2010–2011 Tunisian protests which led to the fall of his government. Since he fled Tunisia, details have gradually come to light of the extent of corruption under his rule. He and his wife Leila Trabelsi, along with their inner circle, are suspected of having pocketed much of the country's wealth over the years and of taking personal stakes in much of the economy. Tunisian Central bank chief stated that Tunisian banks funded businesses linked to the families of the couple to the tune of US\$1.8bio. Videos show that the President stashed cash and jewellery some of which had "historic value" in the president's palace. The total amassed wealth of Ben Ali is unknown to date. However, news media have claimed the wealth of the former leader and his entourage to be estimated at US\$5bio, although they have not detailed how they came to this figure, which thus cannot be verified. The family's interests are thought to include banks, insurance, fishing and construction as well as about 30 properties, including hotels. The interim Tunisian government asked for Interpol to issue an arrest warrant, charging him for money laundering and drug trafficking. On 20 June 2011, Ben Ali and his wife were sentenced in absentia to 35 years in prison.

Country: Tunisia

Key date: 2011 (deposed during Arab Spring)

Muammar Gaddafi & Son

Muammar Muhammed Abu Minyar al-Gaddafi, commonly known as Colonel Gaddafi, was the ruler of the Libyan Arab Republic from 1969 to 1977 and then the "Brother Leader" of the Libyan Arab Jamahiriya from 1977 to 2011, during which he pursued a largely Arab nationalist and Arab socialist philosophy. In 1969, he seized power from King Idris in a bloodless coup, after joining and founding a revolutionary group within the military. Following unsuccessful border conflicts with Egypt and Chad, and Gaddafi's support for foreign militants led to Libya being labelled an "international pariah", with a particularly hostile relationship developing with the US and UK, who accused him of being a dictator and autocrat whose authoritarian administration oversaw multiple human rights abuses and supported international terrorism. For example, in 1981, the new US President Ronald Reagan famously declared Gaddafi an "international pariah" and the "mad dog of the Middle East". He immediately pursued a hard line approach to Libya, considering its government a puppet regime of the Soviet Union. Relations became ever more strained, particularly after Libyan diplomats were accused of shooting dead Yvonne Fletcher, a British policewoman stationed outside their London embassy, in April 1984 and after the US accused Libya of orchestrating the 1986 Berlin discotheque bombing, in which two American soldiers died. Reagan decided to retaliate militarily and in 1986, US military planes launched a series of air-strikes on Libya, bombing

military installations in various parts of the country, killing around 100 Libyans, some of whom were civilians.

One of the targets had been Gaddafi's home in the Bab al-Azizia barracks. In the aftermath of the 1986 US attack, the army was purged of perceived disloyal elements and in 1988, Gaddafi announced the creation of a popular militia to replace the army and police. In 1987, Libya began production of mustard gas at a facility in Rabta, although publicly denied it was stockpiling chemical weapons, and unsuccessfully attempted to develop nuclear weapons. The period also saw a growth in domestic Islamist opposition, formulated into groups like the [Muslim Brotherhood](#) and the [Libyan Islamic Fighting Group](#). Libya stepped up its support for anti-western militants such as the [Provisional IRA](#), and in 1988, [Pan Am Flight 103](#) was blown up over Lockerbie in Scotland, killing 259 passengers. British police investigations identified two Libyans – Abdelbaset al-Megrahi and Lamin Khalifah Fhimah as the chief suspects, and in November 1991 issued a declaration demanding that Libya hand them over. When Gaddafi refused the UN imposed economic sanctions which had deep repercussions for the country's economy. They would only be suspended in 1998 when Libya agreed to allow the extradition of the suspects to the Scottish Court in the Netherlands.

In 2001, Gaddafi condemned the September 11 attacks on the US by Al-Qaeda, expressing sympathy with the victims and calling for Libyan involvement in the War on Terror against militant Islamism. Influenced by the events of the Iraq War, in December 2003, Libya renounced its possession of weapons of mass destruction, decommissioning its chemical and nuclear weapons programmes. Relations with the US improved as a result, while UK Prime Minister Tony Blair met with Gaddafi in the Libyan desert in March 2004 and soon after with the EU in Brussels. The following month, Gaddafi travelled to the EU in Brussels and in 2006 was removed from the US list of state sponsors of terrorism.

After protests against the Libyan government started in February 2011, following the start of the Arab Spring, the UN, the US and EU imposed sanctions again against Gaddafi's regime, and supported rebel groups that led to his downfall and his death in 2011. After the fall of Gaddafi, Libya's interim government the so called National Transitional Council accused Gaddafi and his son Seif al-Islam of using the much of the wealth of the country for their personal use and embezzling billions of dollars. In July 2011 the corruption and human rights non-profit organisation Global Witness published a report on the Libyan Investment Authority, the Country's Sovereign Wealth Fund, and its investments based on a leaked document. According to this report the LIA deposited well over US\$1bio with some major international banks. The LIA not only courted financial institutions but also other bodies in

a bid to garner respectability for example the London School of Economics (LSE) which has an international reputation as one of the world's best universities. Libya's dealings with the LSE called some of its judgments and particularly of those of Sir Howard Davies its Head and a former Head of the UK FSA due to their agreement to accept millions in donations for example a £1.5m Gaddafi International Charity and Development Foundation (GICDF) and to LSE Global Governance (£300,000 received) as well as US\$50,000 paid to the university in return for Sir Howard's advice to Libya's sovereign wealth fund and an award of £2.2mio contract between LSE Enterprise and Libya's Economic Development Board to train Libyan civil servants and professionals. Such was the damage to the reputation of the LSE once these were publicised that it ultimately led to Sir Howard's resignation.⁴

Country: Libya

Key date: 2011 (killed in civil war in Arab Spring)

Muhammad Hosni Mubarak

Mubarak served during three decades as the fourth President of Egypt, from 1981 to 2011. He was elected to his fifth consecutive term as president in September 2005. But the election was the first contested presidential election in Egypt's history, with official results showing Mubarak having won 88.6% of the votes cast. However, civil organisations observing the elections and the Egyptian Organisation for Human Rights reported mass rigging activities, bought votes and fraud. On 25 January 2011, mass protests in Egypt calling for Mubarak's resignation began. Violence in the streets quickly escalated between Mubarak supporters and the opposition following his 1 February 2011, announcement that although he would not seek another term in the presidential elections scheduled for September 2011, he would not resign from his post. On February 10, 2011, protests continued and, Mubarak announced he would be handing over powers to his vice-president, Omar Suleiman, but would remain as president. The following day, Suleiman announced that Mubarak was stepping down and the military's supreme council would run the country.

There are many reasons for the collapse of Mubarak's regime, but one of the most important reason is corruption. Corruption in Egypt had reached unprecedented heights. Reports from Egypt speculated that the personal wealth of Mubarak and his family to be between US\$40bio and US\$70bio due to corruption, kickbacks and legitimate business activities. However, these figures are likely widely inaccurate and cannot be verified. The money was said to be spread out in various bank accounts at home and abroad, and also invested in foreign property though again little has been publicly identified.

Country: Egypt

Key date: 2011 (deposed during Arab Spring)

James Ibori

James Ibori, was Governor of Nigeria's Delta State from 1997 to 2007. In 2012, Ibori pleaded guilty in the UK to ten counts of money laundering and fraud in relation to an estimated US\$250mio of stolen state assets and was sentenced to 13 years imprisonment. Ibori's wife was also been convicted of money laundering. Ibori had an official salary of £4,000 per annum and his formal asset declaration stated that he held no cash or bank accounts outside of Nigeria. Despite this, he bought several houses around the world including one in the UK valued at approximately £2.2mio. The purchase of this house was hidden in a company name called 'Haleway Properties Ltd' which was a previously-formed company incorporated in Gibraltar and had been arranged by his wife, Theresa Ibori, through a UK based fiduciary agent. The beneficial owners of 'Haleway Properties Ltd' were James and Theresa Ibori. The mistress of Ibori was also responsible for the transfer of funds out of Nigeria, investing them on behalf of Ibori, acting as a conduit to pay for properties in the UK. By the end of 2003, his mistress had deposited more than £3mio into a trust fund in Guernsey for the benefit of the Ibori family. The administrators of the trust fund, consistent with the purpose for which it was established, expected that money would be deposited into the account from UK banks. When they received transfers from an unknown Nigerian company called "Sagicon," they conducted further due diligence. Ibori's mistress obtained forged company accounts and incorporation documents, certified by a corrupt solicitor in Nigeria, to falsely show Ibori as a major shareholder of Sagicon.

Ibori and his associates also used multiple UK bank accounts to launder funds. In 2005, Ibori utilised the services of a corrupt London-based solicitor, to launder his funds. Money had been transferred from Nigeria to a UK corporate bank account, which was beneficially owned by Ibori but controlled by his former special assistant. The special assistant transferred some US\$4.7mio from the UK account into a Swiss company account which was beneficially owned by Ibori. Once the funds were held in the account, they were then transferred to yet another Swiss company bank account, which was beneficially owned by another client of the corrupt solicitor. The solicitor then transferred the US\$4.7mio back to one of his client accounts in London, effectively 'washing the money.' Once the money was in the solicitor's client account, it was then deposited into a Texas bank account and used for the deposit on the purchase of a private jet aircraft for Ibori.

Country: Nigeria

Key date: 2012 (guilty of corruption)

Corporates

Lockheed Martin

Lockheed Martin is the world's largest defence contractor. Over the past 40 years, Lockheed has been the subject of major bribery scandals. The payment of bribes, usually via intermediaries and slush funds, were simply once part of doing business.

In the mid-1970s, US Congress investigated foreign payments by US companies revealing allegations and admissions of bribery to foreign government officials and led to the introduction of the FCPA in 1977.

The US Congress investigation included noteworthy mentions of Lockheed Aircraft Corporation bribing senior government officials in Japan and Holland. The Japan case related to payments of US\$1.7mio to then Japanese Prime Minister Tanaka in return for the sale of 21 TriStar planes valued at US\$6.3mio. Lockheed's covert middleman, Yoshido Kodama via a local trading company Marunbeni, provided four lump sum payments to officials over an eight month period including deliveries on 10 August 1973 at the back of the British Embassy in a cardboard box; 12 October 1973, at a phone booth; 21 January 1974 in a hotel parking lot; and 1 March 1974 at an officials' apartment.

The US Senate Committee also learned of US\$1.1mio paid by Lockheed to Prince Bernhard of the Netherlands, then Inspector General of the Dutch Armed Forces and husband of Queen Juliana of the Netherlands, nearly resulting in the abdication of the Queen's position. He renounced his role in exchange for immunity.

Twenty years later, in 1994, Lockheed was investigated by US authorities under the FCPA with respect to paying bribes in Egypt and submitting false statements. Lockheed paid a criminal fine of US\$21.8mio, a civil penalty of US\$3mio and was barred from foreign exports. Lockheed had hired a local consultant and government official, Dr Leila Takla, who was responsible for marketing and sales for Lockheed in Egypt. Lockheed made monthly payments to a company called Takla Inc, whose signatory was Takla's husband.. Dr Takla improperly used her influence with the Ministry of Defence to direct business to Lockheed

Country: US, Japan, Netherlands

Key date: 1973 (LM bribed Japan's then Prime Minister to secure lucrative plane contracts)

Bofors

The name Bofors has been associated with the iron industry for over 350 years. Located in Karlskoga, Sweden, the company originates from the hammer mill "boofors" founded in 1646. A leading Swedish steel producer by the early 1870s, Bofors expanded into weapons manufacture with the first cannon workshop being opened in 1884. Since 1987, Bofors pedigree name also became associated with the murky world of corruption, bribery and unfair trade practices.

The saga began when the Government of India floated a tender in 1984 for buying Howitzer guns for the Indian army. Two providers were shortlisted, the French Sofma and Swedish Bofors. The army tested the two guns and opinions were divided on the quality of the two guns. The chief of the Indian Army, General Sundarji, eventually opted for Bofors and the Government approved the decision in a record 24 hours from receiving the army's recommendation. On 24 March 1986 the contract was awarded to Bofors for the supply of over 400 155mm Howitzer field guns.

Whilst rumours about commissions being paid to the ruling political party for awarding arms deals had been floating for a while, the Bofors scandal first properly surfaced on 16 April 1987, when the Swedish Broadcasting Corporation broke the story that Bofors paid kickbacks to top Indian politicians and key defence officials to secure the deal. The Swedish radio quoted senior Bofors sources as saying that in total, kickbacks of around US\$50mio were paid into the secret Swiss bank accounts of, among others, the then prime minister of India, Mr Rajiv Gandhi.

The Swedish broadcaster insisted it had evidence to back up its report and the scandal picked up steam with the respected Indian daily paper, The Hindu, publishing documents evidencing payments by Bofors to certain questionable companies, namely AE Services. AE Services was shown to be a company which had a paid up capital of Lira 100 and no employees. It was widely alleged that the contract with AE Services specified that payment to AE Services would be made only if the contract for the guns was signed before 30 March 1986.

The media onslaught on Bofors continued and a private diary allegedly belonging to the CEO of Bofors included various code words such as : "Q's" involvement may be a problem due to the closeness with "R". Q's account was at a Swiss Bank where the money from AE Services was paid and was operated by Mr. Ottavio Quattrocchi, an Italian businessman who represented the petrochemicals firm Snamprogetti and was reportedly close to the family of Mr Rajiv Gandhi, allegedly the "R" of the infamous diary. Several other names including the UK-based Hinduja brothers with business interests spread across the media. Mr Win Chadha, a Dubai-based businessman and Mr S.K. Bhatnager, a former Defence Secretary who later served as the Gov-

ernor of Sikkim, were mentioned in the media reports in connection with the burgeoning Bofors scandal.

The unraveling story lost the Government and the ruling party headed by Mr. Rajiv Gandhi its credibility, although Mr Ghandhi always denied it.

After spending years in chasing the accused through domestic and international courts and incurring costs of close to US\$100mio, none of the accused parties in the Bofors matter were convicted. Ironically, the Bofors guns themselves proved to be a success and some say the defining factor, in ensuring India's victory over following conflicts with Pakistan.

Country: Sweden, India

Key date: 1987 (investigations started by Swedish and Indian authorities into allegations of corruption)

Special Focus 6 Thomson CSF - Thales



Thomson CSF now known as Thales is the largest French Defence Company and is associated with a major corruption scandal connected with the sales of Arms to Taiwan. In 1991, the Taiwanese government abruptly ordered the Taiwan Navy to cancel its longstanding commitment to purchase frigates from South Korea and instead purchase a more expensive class of frigates via French company Thomson CSF (now Thales). The contract, valued at US\$2.5bio, was the largest procurement in Taiwan history and also represented a U-turn by France on its foreign policy of not supplying arms to Taiwan.

Employing the services of a local Taiwan agent, Andrew Wang, Thompson CSF arranged kickbacks to persuade the Taiwanese authorities to drop their project with South Korea. The defence contract was heavily inflated and at least US\$26.75mio was paid in kickbacks to Taiwanese politicians and military leaders. Wang was also charged in absentia for the murder of a Taiwan navy Captain Yin, who disappeared the day after representatives from Thomson CSF visited the Taiwan Navy General Headquarters and was believed to have been a whistleblower.

The frigates were delivered but substandard and the Taiwanese would ultimately conclude in 2002,

following a government investigation that the price of the frigate deal had been inflated to FF15bio (US\$2bio) from the original quote of FF10bio, and that Taiwanese politicians and military leaders pocketed us\$26.75mio in kickbacks from the sale. The authorities put the loss incurred by Taiwan from the payment of bribes at US\$520mio (plus interest).

The investigation quickly focussed on Andrew Wang Thomson's agent and accounts blocked in Switzerland following suspicion raised by Swiss Banks. In total, 46 bank accounts were held by Andrew Wang in Switzerland in the names of Andrew Wang, his three sons and a company owned by Wang.

The French side of the frigate affair was no less scandalous. As a result of a broader corruption investigation involving former state owned oil giant Elf Aquitaine, the role of the former foreign minister, Roland Dumas, and his former mistress, Christine Deviers-Joncour, in the frigate deal unraveled. In return for switching foreign policy and approving the contract, Dumas received bribes from Ms Deviers Joncour, who at the time was employed as a lobbyist by Thomson CSF.

Elf was cash-rich at that time and was appointed as the lead public enterprise to help facilitate foreign business of other state-owned companies with generous commissions and bribes. The Elf facilitation team on behalf of Thomson approached Ms Deviers-Joncourt, who persuaded Dumas to approach Mitterrand on the frigate sale. As for herself, Deviers-Joncourt admitted receiving some US\$10mio in commissions from Elf and claims that Elf paid out a total of FF5.5bio (US\$827mio) on behalf of Thomson-CSF (Thales). Ms Deviers Joncour captivated the French public with her book in 1999 titled "The Whore of the Republic", where she detailed gifts she had provided to Dumas in return for his support towards Elf Aquitaine generally, but also the Frigates deal. She also alleged that bribes had been paid to placate China.

In March 2003, Dumas admitted to Le Figaro that France paid US\$500mio in bribes for the frigate deal. Dumas said that the sum was approved by former president Francois Mitterrand, that US\$400mio was paid to the secretary-general of Taiwan's ruling KMT party and that US\$100mio went to the Chinese Communist Party's Central Committee in Beijing. Despite these revelations, the French prosecutors dismissed the case in August 2008 after 7 years of investigations for "lack of evidence". The inquiry had sought to establish whether French politicians, military officials and other middlemen had illegally profited

from the 1991 sale, as it was alleged that substantial parts of this money disappeared into the pockets of various officials.

The finding was hardly surprising given that the French financial judges Renaud van Ruymbeke and Xavière Simeoni claimed at the end of their initial investigation in 2005 that they had repeatedly been denied access to confidential government defence files which were at the heart of the case. This was confirmed when in 2006 the French Consultative Commission on National Defence Secrets (CCSDN) decided not to release documents requested by the investigating magistrates.

Taiwan's navy filed for arbitration with the Paris-based International Court of Arbitration, an offshoot of the International Chamber of Commerce court in 2001 and final judgment was pronounced in May 2010. In an unprecedented ruling the court found that Thales violated the anti-corruption clause in its 1991 contract and spent over US\$500mio on bribes to secure the US\$2.5bio deal to sell six Lafayette class frigates to Taiwan.

More than 20 people, including three senior Taiwan Navy officers were jailed in Taiwan as a result of the frigates scandal. In June 2011 the French government and Thales Group announced that they would pay a fine of €630mio (now about US\$913mio), after losing their appeal against the international court of arbitration ruling for breaching the anti bribery provision in their contract.

As part of the broader corruption scandal in France, Dumas was jailed for six months and forced to resign as head of the French Constitutional Council for receiving illegal funds from Elf Aquitaine while he was foreign minister. Ms Deviers-Joncours was sentenced to three years in prison.

Apart from the death of the naval Captain there are several others who died under mysterious circumstances according to a French investigating magistrate. The Captain's nephew, who was helping to investigate his uncle's death, also died an unusual death, as did a Taiwanese bank official acting for the naval dockyards. Later, Thierry Imbot, a French intelligence agent who had been following the frigate negotiations for the French secret service, fell to his death from his Paris apartment under suspicious circumstances. A year later, a former Taiwan based Thomson employee named Jacques Morrison, who told associates he feared for his life because he was a witness to the talks, also fell or was pushed to his death.

The case though is not yet over. In October 2011 the Taiwanese government filed a US\$98.4mio lawsuit against the French state-owned arms company DCN. The allegations, announced by Taiwan's Defence Minister Kao Hua-chun in Parliament, are also an indication that the French contractors apparently continued with illegal activities well after the original scandal was uncovered. Kao said additional kickbacks prohibited by a 1996 order agreement have been found. Taiwan is seeking the additional penalty for alleged violation of the 1996 agreement, bringing the total to well over US\$1bio

The French government has further problems in other countries because DCN's operations face questions across almost the entire globe, including in Pakistan, Malaysia, India, Saudi Arabia and Chile, with bribes and kickbacks reportedly comprising 8% to 12% of DCN's entire budget and involving political parties and government leaders including former French Prime Minister Edouard Balladur and associates of the former French President Nicholas Sarkozy (who denies all the allegations).

Penalty: US\$913mio (potentially more to come)

Actions: illegal bribes paid to win sale of Navy frigates from France to Taiwan

Country: Taiwan, France

Key date: 2002 (investigations started by Taiwanese authorities into allegations of corruption)

Statoil

Statoil is an Oil company located in Norway. In 2002 and 2003, it paid bribes to an Iranian government official for him to use his influence to assist Statoil in obtaining certain contracts to develop an oil field in Iran and to open doors generally to further work inside Iran.

The bribe was facilitated by the use of a "consulting contract" with an intermediary company organised in the Turks and Caicos Islands and nominally owned by a third party in the UK. The Iranian official, who was described as an advisor to the Oil Minister, and who was not named in the contract, facilitated Statoil's success in obtaining the contract by providing them with non-public business information, including copies of the bid documents from competing companies.

The bribe payments – two payments totaling US\$5.2mio, were effected by wire transfers from Statoil through a US bank account to an account in Switzerland held by a company not named in the contract.

The conduct was discovered in March 2003 during an

internal audit as a result of the payment being made to an entity not involved in the contract, and future payments were suspended in June 2003. The findings were subsequently disclosed in the Norwegian press in September 2003, and Statoil subsequently terminated the contract. Statoil would later agree to the terms of a Deferred Prosecution Agreement with US authorities in 2006.⁵

Country: Norway, Iran

Key date: 2003 (investigations started into bribes paid to Iran)

BAE Systems

BAE Systems Plc (BAE) is the world's second largest defence company and Europe's largest. In 2010, after almost a decade of scrutiny and allegations by the British media and multiple regulatory investigations worldwide, BAE pleaded guilty to criminal charges in the US and agreed to pay US\$400mio fine, one of the largest corporate financial penalties ever imposed in a corporate bribery case.

As part of its guilty plea with the US, BAE also agreed to maintain a compliance programme designed to detect and deter violations of foreign bribery laws and to appoint a compliance monitor for three years.

As a result of the scandal, BAE has also replaced almost all of its top leadership, including its former Chief Executive Officer and Chairman of the Board and overhauled and expanded its Corporate Responsibility efforts.

The UK authorities also fined BAE US\$50mio after it pleaded guilty to a criminal accounting charge. This outcome was widely criticized by anti corruption campaigners, who saw it as a weak outcome after years of investigation into billions of dollars of alleged bribe payments made over years by BAE across Europe, Middle East and Africa. The corruption scandal is one of Britain's most important and politically charged cases.

In 2006, former UK Prime Minister, Tony Blair's government drew heavy criticism for requesting the UK's Serious Fraud Office to drop its case into BAE relating to arms contracts worth billions of pounds, on the grounds of national security. This decision alone compounded by the role of the media and not for profit corruption watchdogs, cemented BAE's place in corporate scandal history and ensured the case had a damaging impact on Britain's reputation regarding its stance against corruption.

The BAE scandal also kickstarted the long overdue

reforms on bribery offences in the UK, leading to the [UK Bribery Act in 2011](#). BAE regularly retained "marketing advisors" to act as intermediaries to assist in the soliciting, promoting and securing of deals. BAE maintained inadequate information on its intermediary advisors namely, who they were and what work they were doing to advance BAE's interests. BAE avoided communicating with its advisors in writing, obfuscating and failing to record the key reasons for the suitability of the advisor or any relevant document pertaining to the work performed. Often, contracts with the marketing advisors were maintained in secret legal trusts in offshore locations.

This conduct served to conceal the existence of payments through BAE's advisors. BAE made payments to these marketing advisors through offshore shell companies beneficially owned by BAE.

BAE also encouraged its marketing advisors to establish their own offshore shell entities to receive payments to disguise the origins and recipients of such payments.

Two examples of payments to marketing advisors which were suspected as questionable were payments of i) more than £19mio to entities associated with an individual, at least some of which was in connection with the promotion or otherwise to secure the leases of Gripen fighter jets from Sweden to the Czech Republic and Hungary and ii) US\$12.4mio made between 1999 and 2005 to Shailesh Vithlani, a Tanzania-based businessman, for his work as an agent in helping to secure a radar deal in Tanzania in 1999.

Country: UK, Czech Republic, Hungary, Tanzania

Key date: 2006 (investigations started by British authorities into allegations of corruption)

Special Focus 7

Siemens



Siemens is a German conglomerate originally founded in 1847. It currently has around 400,000 employees operating in some 190 countries. Beginning in the mid-1990s, Siemens engaged in systematic payments of bribes to win business.

The pattern of bribery by Siemens was unprecedented in scale and geographic reach. The corruption involved more than US\$1.4bio in bribes to government officials in Asia, Africa, Europe, the Middle East and the Americas. Siemens and its subsidiaries in Argentina, Venezuela, France, Turkey, Middle East and in Bangladesh made use of cash desks and slush funds and used numerous persons as conduits to conceal the corrupt payments, describing such payments in the books and records as consulting fees or legal fees.

In 2007 a Bank in Zurich reportedly submitted a suspicious activity report to Swiss law enforcement officials with respect to suspected improper payments by Siemens, who passed the information on to their German counterparts and so the case was uncovered. In 2008, as a result of cases brought by the US DoJ, the US SEC and the Munich Public Prosecutor's Office, Siemens paid a combined total of more than US\$1.6bio in fines, penalties and disgorgement of profits, including US\$800mio to US authorities, making the combined US penalties the largest monetary sanction ever imposed in an FCPA case at that time.

The DoJ and the SEC closely collaborated with the Munich Public Prosecutor's Office in bringing these cases. The high level of cooperation, including sharing information and evidence, was made possible by the use of mutual legal assistance provisions under the 1997 Organisation for Economic Cooperation and Development Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, which entered into force on 15 February 1999.

Siemens was found to be using intermediaries extensively in order to facilitate bribery and corruption and retained a number of "payment intermediaries" whose sole purpose was to transfer money from

Siemens to business consultants. According to the SEC complaint, there were at least 4,283 payments, totalling approximately US\$1.4bio. Some of the consultants were being paid for legitimate consulting services and were subject to business consultant agreements, in addition to the illicit payments.

Other examples of the use of intermediaries were:

- approximately €6mio was paid to employees of ENEL (a partly government-owned Italian power company) in connection with two power plant projects. A Dubai-based business consultant routed the payments through slush funds in Liechtenstein;
- Slush funds were maintained in the name of current and former Siemens employees, third parties or affiliates and bribes were directed through these accounts
- Siemens used sham supplier agreements, receivables and other write-offs to generate payments.

Some 300 people were also investigated by the German authorities and by Siemens itself who also dismissed many senior managers and has sought compensation from 11 board members. The criminal investigations and cases against individuals culminated in April 2010 when a Munich court found Michael Kutschenerreuter, the former financial head of Siemens' telecommunications unit, guilty of breach of trust and abetting bribery. Kutschenerreuter was the most senior Siemens executive found guilty of corruption. He was placed on probation for two years and fined €160,000 (US\$215,300) after admitting that he had covered up slush funds and bribes paid by his employees. The other defendant, Hans-Werner Hartmann, who was in charge of accounting at the company's telecommunications arm, was placed on probation for 18 months and fined €40,000. According to prosecutors, the funds were used to bribe government officials and business contacts to win lucrative contracts in Russia and Nigeria. Siemens announced at the same time as the plea agreement with the DoJ its decision to appoint Theo Waigel, former German finance minister, its first "compliance monitor". Waigel, an architect of German monetary union after the fall of the Berlin Wall, was to report to the US authorities on Siemens' implementation of new compliance measures.

Siemens own internal FCPA investigation was of unprecedented scope with estimated costs exceeding US1bio. It assisted government investigators by providing detailed information from interviews, corporate records, and financial records and routinely shared documents collected overseas that otherwise would be difficult for US authorities to obtain (due to, for example, foreign privacy laws), and provided English translations of documents.

In some instances, Siemens also shared forensic analyses of transactions. Furthermore, Siemens "exported" its cooperation to foreign authorities, including cooperating with the World Bank, the Inter-American Development Bank, and other international development banks to investigate projects that received funding from those banks. It shared the results of that and other investigations with the authorities and cooperated extensively. It took appropriate disciplinary action against individual wrongdoers, including senior management with involvement in or knowledge of the violations. It took remedial action, including the complete restructuring of Siemens AG and the implementation of a sophisticated compliance programme and organisation.

This level of cooperation and the disclosures helped to reduce the ultimate fine which some commentators had thought could be in the region otherwise of US\$5bio.

Penalty: US\$1.6bio

Actions: Illegal systematic bribe paying to secure contracts

Country: Germany and elsewhere

Key date: 2007 (SAR filed in Switzerland starting investigations into bribe paying)

Kellogg Brown & Root

The US government's top contractor in Iraq, KBR, Inc., pleaded guilty in 2009 to bribing high-level officials in the Nigerian government during a decade-long scheme to win more than US\$6bio in overseas construction contracts in connection with the Bonny Island Project in Nigeria. The SEC charged the firms KBR and Halliburton with violating the 1977 Foreign Corrupt Practices Act's anti-bribery provisions and with abuses related to the companies' books, records and internal controls.⁶

KBR and its former parent company, Halliburton, agreed to pay the US government a combined US\$579mio in fines to settle the criminal and civil charges, the most ever paid at that time by a US firm in a foreign corruption case (US\$402mio criminal fine related to the bribery case and the disgorging of US\$177mio in "ill-gotten profits" to the Securities and Exchange Commission under FCPA charges.) Halliburton, which owned KBR before it spun off on its own in 2007, agreed to pay all but US\$20mio of the penalty. In addition to the fines, KBR agreed to hire an independent corporate monitor for the next three years to ensure that the company complied with anti-corruption laws and internal accounting controls.

Mr Jack Stanley former KBR CEO was jailed and fined

US\$10.8mio. KBR was part of a joint venture of four companies, the other three firms involved were not identified -- to build liquefied natural gas facilities on Bonny Island, Nigeria, on Africa's West Coast. The Bonny Island Project involved the development of a very large liquefied natural gas (LNG) processing and transportation facility.

As a result of French, US, and Nigerian investigations, it was revealed that a series of contracts awarded by the Nigerian government, collectively valued at over US\$6bio, were obtained as a result of corrupt payments to Nigerian officials. Specifically, four companies from the US, Japan, France and Italy, formed a joint venture to obtain the Bonny Island contracts, and formed three special purpose Portuguese corporations to engage in operations. The joint venture then employed two intermediaries to bribe government officials. One intermediary formed a Gibraltar corporation, through which US\$130mio of bribe money from the joint venture was funnelled. The second intermediary, a Japanese trading company, received US\$50mio to bribe government officials. The money that moved from the joint venture to the intermediaries was disguised as money received as a result of consulting contracts and moved via wire transfer from accounts in the Netherlands to accounts controlled by the intermediaries in Monaco and Switzerland. The money was ultimately paid to government officials through wire transfers to Swiss accounts controlled by the corrupt officials and by very large cash deliveries, including the delivery of up to US\$1mio in currency at a single time.

At crucial junctures before the contract awards, KBR's then-CEO Albert "Jack" Stanley and others met with members of the Nigerian government to negotiate bribe amounts. Mr. Stanley arranged for US\$182mio in bribes to be paid to senior government officials in Nigeria and to leading executives of a Nigerian energy company controlled by the Nigerian Government.

The only Nigerian official to be named in documents is former President General Sani Abacha. Mr. Stanley arranged for a portion of the bribes to be kicked back into his personal bank accounts.

SEC Chairman Mary Schapiro stated that "Any company that seeks to put greed ahead of the law by making illegal payments to win business should beware that we are working vigorously across borders to detect and punish such illicit conduct."

Key date: 2009 (guilty plea to bribing Nigerian Public Officials to secure lucrative contracts)

Macmillan Publishing

In April 2010, Macmillan Publishing Limited ("MPL") was debarred from participating in World Bank funded tender business for a minimum period of three years after it was established that employees of the company engaged in a scheme in which they gave cash and other items of value to officials of the Ministry of Education, Science and Technology, South Sudan (MOEST) in an effort to influence the officials to ensure that Macmillan was awarded a World Bank contract valued at US\$2.35mio supply of school text books. This influence initially resulted in a request by MOEST to sole source the contract award to MPL, a request which the World Bank refused. Following a subsequent investigation across three East African countries covering the period 2002-2009, it was impossible to be sure that the awards of tenders to the MPL in those jurisdictions were not accompanied by a corrupt relationship. Accordingly, it was plain that the Company may have received revenue that had been derived from unlawful conduct.

The Director of the UK Serious Fraud Office (SFO) took action in the High Court, which resulted in an Order for MPL to pay in excess of £11mio in recognition of sums it received which were generated through unlawful conduct related to its Education Division in East and West Africa. The investigation revealed some of the methods used to establish a relationship with key government officials who were able to influence the outcome of the contract evaluation process in their respective countries. This included the use of local agents or country representatives who received payments transferred to private and business bank accounts which were then withdrawn in cash and paid to government officials. In addition to this other bribery methods such as gifts, for example, travel and holidays, were also used.

Country: US, South Sudan

Key date: 2010 (Macmillan debarred by World Bank due to bribe paying)

Special Focus 8 GlaxoSmithKline



In 2012 a Federal Judge in Boston approved a plea agreement between the US Food and Drug Administration and GlaxoSmithKline ("Glaxo") to pay a US\$3bio fine for criminal and civil violations relating to health care fraud involving 10 drugs manufactured by Glaxo.⁷ The fine was considered the largest settlement involving a

pharmaceutical company. US federal prosecutors had charged the British drug maker with illegally marketing drugs not approved by the FDA (anti-depressants) and withholding safety data from US Regulators relating to the drug Avandia, which was found to increase heart attacks and congestive heart failure.

The case stemmed from claims made by four employees of Glaxo which tipped off US federal investigators that the company was engaging in a number of improper practices for a period that spanned more than five years (late 1990 to the mid 2000s). These practices included providing lavish hospitality, such as all-expense paid trips to Bermuda, Jamaica and California, and other kickbacks to doctors who promoted the sale of the drugs for unapproved uses.

For example, in 2000 and 2001, Glaxo held eight lavish three day events in Puerto Rico, Hawaii and Palm Springs including providing US\$750 in spending money, free board and lodging and access to deep sea fishing, golfing and rafting in an effort to persuade doctors to prescribe the various anti-depressants to patients. Airfares were also covered for doctors and their spouses and speakers at the events were paid as much as US\$2,500 for one hour sessions up to three times per day. Glaxo paid one speaker in particular up to US\$1.5mio over a three year period to promote the drug Wellbutrin, again for unapproved uses. Misleading articles were also prepared and given by sales reps to doctors to secure more business. One doctor wrote "Dinner and a Yankee game with family. Talked about Paxil studies in children." The false reports used by Glaxo employees were published and used despite knowing that three trials had failed to prove the drug was effective for children.

Sales reps were encouraged to push Glaxo drugs and were given an expense account of up to US\$600,000 for entertaining doctors. The events included providing regular golf lessons, taking potential clients on fishing trips and to Nascar race days and other sporting events, and providing tickets to Madonna concerts.

The case was prosecuted under the US False Claims Act which penalizes those who commit fraud and rewards those who report it.

Country: US

Penalty: US\$3bio

Actions: illegal activities regarding the sales of drugs

Key date: 2012 (GSK pleaded guilty to US false Claims Act violations and also admitted essentially to paying bribes)

Environmental Crime

Seveso

In 1976 an explosion occurred in a chemical reactor in the ICMESA chemical company in Meda, Italy, not far from Seveso, a neighboring town. A toxic cloud was released containing high concentrations of a highly toxic form of dioxin. Health effects were immediately recognised as a consequence of the disaster and victims were compensated. A long-term plan of health monitoring has been put into operation. Seveso victims suffered from a directly visible symptom known as chloracne, affecting the skin but also from genetic impairments.

The Seveso accident and the immediate reaction of authorities led to the introduction of European regulation in 1982 for the prevention and control of accidents involving toxic substances. This regulation is now known as the Seveso Directive, which is a mainstay for European countries to manage industrial safety. It obligates appropriate safety measures, and also public information on major industrial hazards, which is now known as the 'need to know' principle. Interestingly local and regional authorities had no idea the plant was a source of risk. The factory had produced its goods for more than 30 years but the local authorities as well as the public had little idea of the nature of the operation and the potential dangers.

Country: Italy
Key Date: 1976

Bhopal

The Bhopal disaster, also referred to as the Bhopal gas tragedy is classified as the world's worst industrial catastrophe and man-made environmental disaster which took place in the late night hours of 2-3 December 1984 in Bhopal, Madhya Pradesh, India at the Union Carbide India Limited (UCIL) pesticide plant. The UCIL was an Indian subsidiary of the Union Carbide Corporation (UCC), Indian Government controlled banks and the Indian general public controlled a 49.1% share of the UCIL. The disaster was a leak of methyl isocyanate (MIC) gas and other various chemicals from the plant which resulted in exposure of the chemicals to several thousand people. The death toll estimate counts vary, but official estimates indicate the immediate death toll as 2,259 and the government of Madhya Pradesh has officially confirmed 3,787 deaths related to the accidental gas leak. Other estimates by government agencies estimate 15,000 deaths, whilst another estimates 8,000 deaths within the first several weeks of the leak and another 8,000 from gas leak exposure related diseases since the accident.

In 2006, the government released an affidavit stating that the gas leak caused 558,125 injuries including 38,478 temporary partial and approximately 3,900 severely and permanent disabling injuries. The cause of

the leak was water entering a tank containing 42 tons of methyl isocyanate or MIC, which created an exothermic reaction which increased the temperature inside the tank to over 200°C or 392°F, and raised pressure inside the tank resulting in the venting of toxic gases into the atmosphere, and ultimately being blown by northwesterly winds over Bhopal. There are differing theories on what transpired to cause the water to get into the MIC tank, varying from maintenance to sabotage

Country: India
Key Date: 1984

Chernobyl

In 1986 tests were conducted in nuclear reactor 4 of the Chernobyl nuclear power plant in Ukraine, located 80 miles from Kiev. These tests required part of the security system to be shut down. The tests however caused the cooling water to start boiling, which accelerated with temperatures reaching more than 2000°C in the reactor, melting fuel rods and further cooling water boiling. Steam escaped from pressures in water cooling pipes which resulted in cracks, which caused an explosion, blowing off the roof of the reactor, starting a major fire and simultaneously forming an atmospheric radioactive cloud instantly killing 31 people. The following day over 135,000 people were permanently evacuated from within a 30kms radius of the accident. This area was labelled the "special zone" as the high levels of radioactivity have been predicted to exist for several centuries. The radioactive cloud soon blew north and northwest, with the cloud covering a large area of Northern Europe, as far as the Netherlands, causing fresh fruit and vegetable consumption to be prohibited. After much discussion the entire Chernobyl nuclear power plant was finally closed in 2000, despite the fact that Ukraine derived 5% of its power supply from the power plant.

The World Health Organisation (WHO) stated that approximately 800,000 people worked on restoring the reactor and cleaning up pollution in the first year after the accident, with risks to health obvious, albeit many only worked for short periods of time. Ukrainian government figures show that more than 8,000 Ukrainians have died as a result of exposure to radiation during the first cleanup operation. It is stated that the eventual death toll resulting from the nuclear explosion may end up as high as 300,000-400,000, with increases in cancers also in neighboring countries, particularly in Belarus. The numbers that will ultimately be affected by the Chernobyl disaster has been estimated as high as 11 times that of the cancer deaths expected from the combined 1945 bombings of Hiroshima and Nagasaki. Today it is believed that over 4 million people in the Ukraine, Belarus and Western Russia still live on contaminated ground.

Country: Ukraine
Key Date: 1986

Fraudsters

Accounting Fraudsters

Alan Bond

Alan Bond could perhaps be regarded as one of the most controversial figures in Australian public life. Born in the UK, Bond rose from being a sign painter to the chairman of one of Australia's largest listed companies, Bond Corporation. Bond achieved cult status in Australia for his role in financing Australia's America's Cup challenge in 1983 which saw the Cup leave America's shores for the first time. This achievement aside, Bond through his activities in Bond Corporation was involved in what is still perhaps Australia's largest corporate fraud. Bond Corporation was listed on the Australian Securities Exchange and during the late 1980s experienced cash flow problems. To address this and following the fall of global stock markets in 1987, which provided the opportunity, Bond Corporation moved to acquire listed Bell Group which possessed the real prize, a cash rich subsidiary, Bell Resources.

Three individuals including Alan Bond, Tony Oates and Peter Mitchell set about to strip Bell Resources of its cash transferring monies directly from Bell Resources to or for the use of Bond Corporation in contravention of Australian company law. The offences included failing to act honestly as a company director with intention to defraud, conspiracy to defraud and improper use of their positions as a company directors. Ultimately A\$1bio was drawn from the company and routed to a number of Bond controlled entities. Ultimately the asset stripping was in vain, Bond Corporation was declared insolvent in 1991 and the three individuals charged and convicted. Bond and Mitchell sentenced to 4 years jail and Oates to 5 years.

The ability to both trace and retrieve the stolen assets possessed by Bond has been hampered for many years according to his trustee in bankruptcy by the use of quite sophisticated corporate structuring in multiple jurisdictions, use of fiduciary representatives in secrecy jurisdictions and companies issuing bearer shares, all of which have been designed to distance Bond being identified with them. As an aside, Bond has returned to corporate life, albeit in Britain and has been associated with several proposed start-up companies, none of which has yet been able to access the public markets.

Company: Bell Resources

Country: Australia

Key date: 1991 (charged with corporate fraud)

Robert Maxwell

On 5 November 1991, at the age of 68, Maxwell was sailing on his luxury yacht, the Lady Ghislaine, cruising off the Canary Islands. His global business empire was seriously overextended and he had taken illegally hundreds of millions of pension fund assets, to support his ailing companies. Banks and financial investigators in London were closing in and one had referred that very day their concerns with evidence to Britain's Serious Fraud Office. Maxwell was informed and at some stage that day he fell off the boat, his body subsequently being found floating in the Atlantic Ocean. The official ruling was death by accidental drowning. Some commentators have alleged suicide, others that he was murdered.

Robert Maxwell was born Ján Ludvík Hoch into a poor Yiddish-speaking Jewish family in a small town in Czechoslovakia. Most members of his family died in Auschwitz during the second world war, but he himself escaped, arriving in Britain in 1940 as a 17-year-old refugee. Maxwell joined the British Army in 1941. He was involved in action across Europe from the Normandy beaches to Berlin. In January 1945 he received the Military Cross from Field Marshal Montgomery. It was during this time that British Intelligence changed his name several times, finally settling on Ian Robert Maxwell. In 1945 he married and with his wife Betty had nine children.

After the war, Maxwell worked as a newspaper censor for the British military command in Berlin. Later, he used various contacts in the Allied occupation authorities to go into business, becoming the British and US distributor for Springer Verlag, a publisher of scientific books. In 1951 he bought three quarters of Butterworth-Springer, a minor publisher. They changed the name of the company to Pergamon Press and rapidly built it into a major publishing house.

In 1964, representing the Labour Party, he was elected as Member of Parliament (MP) for Buckingham. He was re-elected in 1966, but lost in 1970.

Maxwell established the Maxwell Foundation in Liechtenstein in 1970. In 1974 he acquired the British Printing Corporation (BPC) and changed its name Maxwell Communications Corporation. By the 1980s Maxwell's various companies owned the popular UK titles, Daily Mirror, the Sunday Mirror, the Scottish Daily Record and Sunday Mail and several other newspapers, Pergamon Press, Nimbus Records, Collier books, Maxwell Directories, Prentice Hall Information Services, Macmillan (US) publishing, and the Berlitz language schools. He also owned a half-share of MTV in

Europe and other European television interests, Maxwell Cable TV and Maxwell Entertainment.

Maxwell was also well known as the chairman of Oxford United Football Club, saving them from bankruptcy and leading them into the top flight of English football, winning the League Cup in 1986. Maxwell bought into Derby County FC in 1987.

It was through Maxwell's purchase of Macmillan Inc the American publishing firm, for US\$2.6bio, which by some estimates was over three times its value, which put the Maxwell empire into financial distress. As a result of overextending his group, he was forced to sell his successful Pergamon Press and Maxwell Directories to Elsevier for £440mio though he used some of this money to buy the ailing New York Daily News.

Maxwell was given a funeral in Israel better befitting a head of state than a publisher. On 10 November 1991, Maxwell's funeral took place on the Mount of Olives in Jerusalem, across from the Temple Mount. It was attended by the country's government and opposition leaders. No fewer than six serving and former heads of the Israeli intelligence community listened as Prime Minister Yitzhak Shamir eulogized: "He has done more for Israel than can today be said." It has been hinted that Maxwell's service to the Israeli state related to his role in persuading the Czech government in 1948 to arm Israel in their War of Independence that year. Czech military assistance was both unique and crucial for the fledgling state as it battled for its existence. It was Maxwell's covert help in smuggling aircraft parts into Israel that led to the Jewish state having air supremacy during their 1948 War of Independence. Jewish leaders were also grateful for Maxwell's intervention and material help in securing the freedom and immigration between 1988–1991 of over one million Russian Jews through his friendship with Mikhail Gorbachev.

Maxwell's death triggered a flood of claims with banks frantically calling in their massive loans, estimated at over US\$4.5bio. Following the shock that the Maxwell empire was broke and couldn't repay its debts, came the even more shocking discovery that Maxwell had illegally pledged the same assets as collateral for various loans, for example, Maxwell had secretly, "borrowed" US\$767mio from his employees pension funds at the two public companies under his control.

His two sons Kevin and Ian struggled to hold the empire together, but were unable to prevent its collapse. The essence of Maxwell's crime was simple. On the one hand, he had companies where he owned 50-70% of the capital and whose shares were publicly quoted on

the stock exchange; the employees of these companies subscribed to a company pension fund. On the other hand, he had private companies. What he did was to siphon off cash and assets from the public companies and from their pension funds into the private ones which were in financial distress.

He also siphoned off cash borrowed from financial institutions, from intended companies and away from promised purposes. For example, Maxwell purchased an investment fund, First Tokyo Index Trust, (FTIT), a UK listed investment trust in the summer of 1999 as the Maxwell empire was in deep financial distress, though this was only known by Maxwell himself. Through Headington Investments, a finance company under his control, Maxwell borrowed \$100 million from Swiss Bank Corp. to buy the entire First Tokyo portfolio, which owned a broad based selection of marketable securities. The transaction was complex due to English law requirements, but in essence, Maxwell was given the money to purchase FTIT in exchange for his promise to provide collateral for the loan by securing the marketable securities in favor of the lender. The collateral couldn't be provided whilst FTIT was a listed company as English Law prohibited such action, so it was agreed as part of the loan that once purchased FTIT would be delisted and then as a private company the collateral would be provided. The time period from providing Maxwell with the funding and the Swiss Bank receiving the collateral was estimated at around 6-8 weeks. Following the acquisition of FTIT, and in breach of his agreement with the Swiss Bank, Maxwell pledged the securities owned by First Tokyo to other Lenders who had been pressurizing Maxwell over their loans to other Maxwell Companies. When delays were reported and the collateral didn't arrive, and alternative collateral also failed to materialize, and when the Swiss Bank realised that its collateral had been pledged to third parties, it informed Maxwell that it was notifying the UK police and Serious Fraud Office. The date of this message and notification coincided with the date Maxwell fell from his luxury yacht, the Lady Ghislaine.

Eventually, the pension funds were mostly replenished with monies recovered from investment banks, Lehman and Goldman Sachs, as well as contributions from the British government and creditors recovered some of their assets. The result was that, in general, pensioners received about 50% of their company pension entitlement. The Maxwell companies filed for bankruptcy protection in 1992. His son, Kevin Maxwell was declared bankrupt with debts of £400mio. In 1995 Maxwell's sons Kevin and Ian and two other former directors went on trial for conspiracy to defraud, but were unanimously acquitted by a twelve man jury in

1996.

It is 20 years now since Maxwell fell from his yacht and drowned. Maxwell was clever, self-confident, forceful and, on occasion charming. His fraudulent activities were carried out intelligently, tenaciously, ruthlessly. They involved famous businesses in Britain the Daily Mirror, the Sunday Mirror, the Daily Record and in the US the New York Daily News and the Macmillan publishing group.

The account written by UK government DTI inspectors into the affair provide a valuable insight into how Maxwell systematically plundered both the non-family shareholders in his businesses and the company pension funds and provide lessons for the future.

Maxwell was very secretive. His objective was to prevent anybody having a full picture of his activities. Only Maxwell himself knew how everything fitted together. He engaged in deceit by confusion. His private companies were given different financial years, constantly lent and borrowed to and from each other and transferred assets between themselves all so that the bankers lending to these entities would never be able to see clearly what was going on.

Certain decisions must be ratified by a company's directors. So all companies, public and private, must hold board meetings. When he couldn't avoid them, Maxwell called them at short notice, provided the necessary documents only a few minutes before and taking back the papers as soon as the meeting was over. If, as was necessary in the public companies, a board meeting had long been scheduled, then it would be postponed at the last moment and be re-arranged with the result that often only a few directors could attend.

If secrecy was Maxwell's rule number one, then securing all power into his own hands came next. He made sure that he was the only director able to sign cheques for more than a trifling amount. On the same evening that Maxwell acquired control of Mirror Group Newspapers, he went to the Mirror Building in Holborn, London, and ordered that a board meeting be summoned. It took place at 2.45am. Maxwell obtained agreement that he had the authority to sign cheques and make transfers from the company's bank accounts on his sole signature for any amount. In effect, he had picked the lock on the company safe.

A second method of securing power was to get the directors of the public companies to agree that the entire powers of the board be delegated to him as a committee of one. He told board members that this was necessary because he was often abroad when quick decisions were

needed. Actions taken would be reported to the next meeting of the board so that they could be ratified.

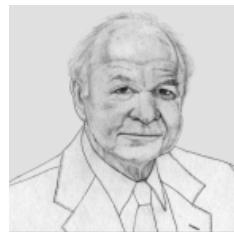
The third element in Maxwell's technique was to wear the cloak of respectability at all times. He was able to get top class advisers, lawyers, accountants and bankers, as well as establishment figures to work with him. He also courted leading statesmen around the world.

Company: Maxwell Communications Corp PLC

Country: UK

Key date: 1991 (Maxwells unexplained sudden death leads to unravelling of major corporate fraud)

Special Focus 9 Ken Lay & Others



On 5 March 2001 Bethany McLean a financial journalist working for Fortune magazine was the first to seriously question the financial performance of one of Americas most successful Companies, Enron Corp. Enron was created in 1985, through

the merger of two Texas based natural gas pipeline companies, Houston Natural Gas and InterNorth, by Ken Lay. In the early 1990s, pushed by the likes of Enron, the US Congress passed legislation deregulating energy markets, which then made it possible to sell energy at higher prices, significantly increasing revenues for those involved. By 1992 Enron rose to become the largest seller of natural gas in North America as well as acquiring and operating a variety of assets including electricity plants, pulp and paper plants, water plants, and broadband services. The corporation also gained additional revenue by trading contracts for the same array of products and services it was involved in. Enron's stock rose from the start of the 1990s until year-end 1998 by 311%. The stock increased by 56% in 1999 and a further 87% in 2000, compared to a 20% increase and a 10% decline for the index during the same years. By 31 December 2000, Enron's stock was priced at US\$83.13 and its market capitalization exceeded US\$60bio, 70 times earnings and six times book value. Bethany Mclean in her article, "Is Enron Overpriced?" pointed out though that analysts and investors did not know how Enron was earning its income, that she found "strange transactions", "erratic cash flow", and "huge debt."⁸ Whilst Enron reacted aggressively but

without substantive answers, others began to raise questions over the summer of 2001. The price of the stock began to fall.

On August 14, 2001 then CEO Jeffrey Skilling announced he was resigning his position as CEO after only six months.⁹ Skilling had long served as president and COO under now Chairman and then CEO Ken Lay before himself being promoted to CEO. Skilling cited personal reasons for leaving the company. Skilling had recently sold 450,000 shares of Enron at a value of around US\$33mio. Ken Lay, assured stunned market watchers that there would be "no change in the performance or outlook of the company going forward" from Skilling's departure. On 15 August, Sherron Watkins, vice president for corporate development, sent an anonymous "whistleblowing" letter to Ken Lay warning him about the company's accounting practices, stating for example, that "I am incredibly nervous that we will implode in a wave of accounting scandals," though this warning whilst internally investigated was essentially rejected.¹⁰

On 2 December 2001, Enron sought Chapter 11 protection. It was the largest bankruptcy in US history (before being surpassed by WorldCom's bankruptcy the following year), and resulted in 4,000 lost jobs. The day that Enron filed for bankruptcy, the employees were told to pack up their belongings and were given 30 minutes to vacate the building. Nearly 62% of 15,000 employees' savings plans relied on Enron stock that was purchased at US\$83 in early 2001 and was now practically worthless. On 17 January 2002 Enron fired Arthur Andersen as its auditor, citing its accounting advice and the destruction of documents. Andersen countered that they had already severed ties with the company when Enron entered bankruptcy.

It quickly became clear that the Company's financial statements significantly inflated revenues and asset prices and hid debts off the Enron balance sheet. According to McLean and Elkjaer in their book *The Smartest Guys in the Room*, "The Enron scandal grew out of a steady accumulation of habits and values and actions that began years before and finally spiraled out of control."¹¹ The combination of these habits, values and actions led to the bankruptcy of the company in late 2001. Enron's US\$63.4bio in assets made it the largest corporate bankruptcy in US history until WorldCom's bankruptcy the following year. Enron Chairman and founder Ken Lay, CEO, Jeffrey Skilling, and CFO Andrew Fastow, together with other executives, constantly focused on meeting Wall Streets quarterly expectations. Enron used unethical practices including questionable accounting practices to misrepresent and to portray a favorable

depiction of its financial performance, particularly with respect to overbooking revenues and hiding debt. Examples of unlawful and unethical practices included booking Future Revenues upfront and the use of special purpose vehicles to hide mounting debt to circumvent accounting conventions. The Enron bankruptcy also led to the dissolution of Arthur Andersen, which was one of the five largest audit and accountancy partnerships in the world, who were both misled but also pressurised by Enron to ignore certain issues.

Fastow and his wife, Lea, both pleaded guilty to charges against them. Fastow was initially charged with 98 counts of fraud, money laundering, insider trading, and conspiracy, among other crimes. Fastow pleaded guilty to two charges of conspiracy and was sentenced to ten years with no parole in a plea bargain to testify against Lay, and Skilling. Lea was indicted on six felony counts, but prosecutors later dropped them in favor of a single misdemeanor tax charge. Lea was sentenced to one year for helping her husband hide income from the government.

Lay and Skilling went on trial for their part in the Enron scandal in January 2006. The 53-count, 65-page indictment covers a broad range of financial crimes, including bank fraud, making false statements to banks and auditors, securities fraud, wire fraud, money laundering, conspiracy, and insider trading. On 25 May 2006, the jury in the Lay and Skilling trial returned its verdicts. Skilling was convicted of 19 of 28 counts of securities fraud and wire fraud and acquitted on the remaining nine, including charges of insider trading. He was sentenced to 24 years and 4 months in prison. Lay pleaded not guilty to the eleven criminal charges, and claimed that he was misled by those around him. He attributed the main cause for the company's fall to Fastow. Lay was convicted of all six counts of securities and wire fraud for which he had been tried, and he faced a total sentence of up to 45 years in prison. However, before sentencing was scheduled, Lay died on 5 July 2006. At the time of his death, the SEC had been seeking more than US\$90mio from Lay in addition to civil fines. The case surrounding Lay's wife, Linda, is a difficult one. She sold roughly 500,000 shares of Enron ten minutes to thirty minutes before the information that Enron was collapsing went public on 28 November 2001. Linda was never charged with any of the events related to Enron. All told, sixteen people pleaded guilty for crimes committed at the company, and five others, including four former Merrill Lynch employees, were found guilty. Eight former Enron executives testified the star witness being Fastow against Lay and Skilling, his former bosses. Another was Kenneth Rice, the former chief of Enron Corp's high-speed Internet unit,

who cooperated and whose testimony helped convict Skilling and Lay. In June 2007, he received a 27-month sentence.

Arthur Andersen was charged with and found guilty of obstruction of justice for shredding the thousands of documents and deleting e-mails and company files that tied the firm to its audit of Enron. Although only a small number of Arthur Andersen's employees were involved with the scandal, the firm was effectively put out of business; the SEC is not allowed to accept audits from convicted felons. The firm surrendered its CPA license on 31 August 2002, and 85,000 employees lost their jobs. The conviction was later overturned by the US Supreme Court due to the jury not being properly instructed on the charge against Andersen. The Supreme Court ruling theoretically left Andersen free to resume operations. However, the damage to the Andersen name had been so great that it has not returned as a viable business even on a limited scale.

Enron's shareholders lost US\$74bio in the four years before the company's bankruptcy (US\$40 to US\$45bio was attributed to fraud). As Enron had nearly US\$67bio that it owed creditors, employees and shareholders received limited, if any, assistance aside from severance from Enron. To pay its creditors, Enron held auctions to sell assets including art, photographs, logo signs, and its pipelines. More than 20,000 of Enron's former employees in May 2004 won a suit of US\$85mio for compensation of US\$2bio that was lost from their pensions. From the settlement, the employees each received about US\$3,100. The following year, investors received another settlement from several banks of US\$4.2bio. In September 2008, a US\$7.2bi settlement from a US\$40bi lawsuit, was reached on behalf of the shareholders. The settlement was distributed among the lead plaintiff, University of California (UC), and 1.5 million individuals and groups. UC's law firm Coughlin Stoia Geller Rudman and Robbins, received US\$688mio in fees, the highest in a US securities fraud case. At the distribution, UC announced in a press release "We are extremely pleased to be returning these funds to the members of the class. Getting here has required a long, challenging effort, but the results for Enron investors are unprecedented."

Enron management was extensively compensated using stock options, similar to other US and non-US companies. This setup of stock option awards caused management to create expectations of rapid growth in efforts to give the appearance of reported earnings to meet Wall Street's expectations. The stock ticker was located in lobbies, elevators and on company computers. At budget meetings, Skilling would develop

target earnings by asking "What earnings do you need to keep our stock price up?" and that number would be used, even if it was not feasible. At 31 December 2000, Enron had 96 million shares outstanding under stock option plans (approximately 13% of common shares outstanding). Enron's proxy statement stated that, within three years, these awards were expected to be exercised. Using Enron's January 2001 stock price of US\$83.13 and the directors' beneficial ownership reported in the 2001 proxy, the value of director stock ownership was US\$659mio for Lay, and US\$174mio for Skilling. Skilling believed that if employees were constantly cost-centred, it would hinder original thinking. As a result, extravagant spending was rampant throughout the company, especially among the executives. Employees had large expense accounts and many executives were paid sometimes twice as much as competitors. In 1998, the top 200 highest-paid employees received US\$193mio from salaries, bonuses, and stock. Two years later, the figure jumped to US\$1.4bio.

Enron's auditor firm, Arthur Andersen, was accused of applying reckless standards in their audits because of a conflict of interest over the significant consulting fees generated by Enron. In 2000, Arthur Andersen earned US\$25mio in audit fees and US\$27mio in consulting fees (this amount accounted for roughly 27% of the audit fees of public clients for Arthur Andersen's Houston office). The auditors' methods were questioned as either being completed solely to receive its annual fees or for their lack of expertise in properly reviewing Enron's revenue recognition, special entities, derivatives, and other accounting practices. Enron hired numerous Certified Public Accountants (CPA) as well as accountants who had worked on developing accounting rules with the Financial Accounting Standards Board (FASB). The accountants looked for new ways to save the company money, including capitalizing on loopholes found in Generally Accepted Accounting Principles (GAAP), the accounting industry's standards. One Enron accountant revealed "We tried to aggressively use the literature [GAAP] to our advantage. All the rules create all these opportunities. We got to where we did because we exploited that weakness."

Between December 2001 and April 2002, the Senate Committee on Banking, Housing, and Urban Affairs and the House Committee on Financial Services held multiple hearings about the collapse of Enron and related accounting and investor protection issues. These hearings and the corporate scandals that followed Enron led to the passage of the Sarbanes-Oxley Act on 30 July 2002.¹² The Act is nearly "a mirror image of Enron: the company's perceived corporate governance

failings are matched virtually point for point in the principal provisions of the Act." The main provisions of the Sarbanes-Oxley Act included the establishment of the Public Company Accounting Oversight Board to develop standards for the preparation of audit reports; the restriction of public accounting firms from providing any non-auditing services when auditing; provisions for the independence of audit committee members, executives being required to sign off on financial reports, and relinquishment of certain executives' bonuses in case of financial restatements; and expanded financial disclosure of firms' relationships with unconsolidated entities. On 13 February 2002, due to the instances of corporate malfeasances and accounting violations, the SEC called for changes to the stock exchanges' regulations. In June 2002, the New York Stock Exchange announced a new governance proposal, which was approved by the SEC in November 2003. The main provisions of the final NYSE proposal include: All firms must have a majority of independent directors; independent directors must comply with an elaborate definition of independent directors. The compensation committee, nominating committee, and audit committee shall consist of independent directors. All audit committee members should be financially literate. In addition, at least one member of the audit committee is required to have accounting or related financial management expertise and in addition to its regular sessions, the board should hold additional sessions without management .

The following are examples of some notable transactions of interest: Booking Future Revenues upfront - For one contract, in July 2000, Enron and Blockbuster Video signed a 20-year agreement to introduce on-demand entertainment to various US cities by year-end. After several pilot projects, Enron recognised estimated profits of more than US\$110mio from the deal, even though analysts questioned the technical viability and market demand of the service. When the network failed to work, Blockbuster pulled out of the contract. Enron continued to recognise future profits, even though the deal resulted in a loss. Enron used special purpose vehicles to hide its mounting debt to circumvent accounting conventions and by 2001 had hundreds of such vehicles. Examples looked into by the US Senate in January 2002 and the subject of a Report were SPVs or transactions known as Fishtail, Bacchus, Sundance, and Slapshot.¹³ These four transactions took place in Q1 and Q2 2001 and were all related to Enron's electronic trading business in the pulp and paper industry - a new business being developed by Enron. The senate found that none of the transactions could have been completed without the backing and active participation of a major financial institution willing to facilitate a

client's deceptive accounting or tax transactions. The evidence compiled in the Report and hearings indicated that major US financial institutions deliberately misused structured finance techniques to help Enron engage in deceptive accounting or tax strategies, being rewarded with millions of dollars in fees or favorable consideration in other business dealings.

The Senate subcommittee found that all four transactions "reflected efforts by Enron to keep debt off its balance sheet or to manufacture immediate returns" to artificially improve financial results for 2000 and 2001. Three of the transactions were categorised as "sham asset sales" - ie transfers of assets at inflated values from Enron to Special Purpose Entities ("SPEs") or joint ventures that Enron orchestrated where essentially the required independence or risk to funds to did not exist. Essentially they allowed Enron to create a disguised 6 month loan from Citigroup. The fourth transaction was categorised as a "sham loan" - of US\$1bio advanced by Chase to obtain around US\$60mio in tax benefits and around US\$65mio of financial statement benefits to Enron. The Sub-committee's findings showed that in each transaction it is apparent that the financial institutions involved often had reservations regarding the transactions and either internal systems failed ultimately to give effect to these reservations, or financial reward was deemed sufficient to outweigh the perceived risks. For example, relating to Citigroup's involvement in the "Sundance" transaction: "Just prior to the closing for the Sundance transaction, three senior Citigroup officials strongly warned against proceeding with the deal, in part due to its "aggressive" accounting. The head of Citigroup's Risk Management team for the Global Corporate and Investment Bank stated in a memorandum sent to the head of the investment bank "This is a follow-up to our lunch conversation on the transaction for Enron. If you recall, this is a complex structured transaction, which I have refused to sign off on. Risk Management has not approved this transaction for the following reasons: ... The GAAP accounting is aggressive and a franchise risk to us if there is publicity (a la Xerox)." In an accompanying email, the head of Citigroup's Global Relationship Bank wrote "We ([the Global Energy and Mining group head] and I) share Risk's view and if anything, feel more strongly that suitability issues and related risks when coupled with the returns, make it unattractive. It would be an unfortunate precedent if both GRB relationship management and Risk's views were ignored." Despite these strongly worded warnings from senior personnel the transaction went forward on 1 June 2001. In testimony to the sub committee and although Citigroup internal policy requires signed management transaction approvals for transactions as

large as Sundance, Citigroup could not locate any of the normal signed approvals.

The second case relates to Chase's role in the "Slapshot" transaction: In relation to this transaction, the Subcommittee noted that: "Chase was paid more than US\$5mio for designing and orchestrating Slapshot. Enron could not have completed this transaction without the initiative and enthusiastic backing of a major financial institution with the resources to issue and move a US\$1bio daylight overdraft through multiple bank accounts across international lines in a single day. Without Chase's willing efforts to design, fund, and execute the incredibly complex transactions involved, whose details had to be carefully planned and co-ordinated, Enron would not have been able to make use of this deceptive tax strategy."

Company: Enron

Penalty: Top management arrested on fraud charges
Actions: Systemic corporate fraud and manipulations
Country: US
Key date: 2001 (Enron filed for bankruptcy, largest at that time)

Bernie Ebbers

Bernie Ebbers was the CEO of WorldCom which at its height, was the US's second largest long distance phone company (after AT&T). WorldCom grew largely by aggressively acquiring other telecommunications companies, most notably MCI Communications. On 5 October 1999 Sprint Corporation and MCI WorldCom announced a US\$129bio merger agreement between the two companies. Had the deal been completed, it would have been the largest corporate merger in history, ultimately putting MCI WorldCom ahead of AT&T. However, the deal did not go through because of pressure from the US Department of Justice and the EU on concerns of it creating a monopoly. On 13 July 2000, the boards of directors of both companies acted to terminate the merger. Later that year, MCI WorldCom renamed itself to simply "WorldCom".

Only 2 years later, on 21 July 2002, WorldCom filed for Chapter 11 bankruptcy protection in the largest such filing in US history at the time (since overtaken by the collapse of Lehman Brothers and Washington Mutual in September 2008). The WorldCom bankruptcy proceedings followed that of Enron which was, up until WorldCom, the largest bankruptcy.

In 2000, the telecommunications industry entered a downturn and WorldCom's aggressive growth strategy suffered a serious setback, particularly following its abandoned deal with Sprint. By September 2000,

WorldCom's stock was declining and Bernard Ebbers, the Company's CEO came under increasing pressure from banks to cover margin calls on his personal WorldCom stock that was used to finance his other business interests (timber and yachting, among others).

During 2001, Ebbers persuaded WorldCom's board of directors to provide him corporate loans and guarantees in excess of US\$400mio to cover his margin calls. The board hoped that the loans would avert the need for Ebbers to sell substantial amounts of his WorldCom stock, as his doing so would put further downward pressure on the stock's price. However, this strategy ultimately failed and Ebbers was ousted as CEO in April 2002.

Beginning modestly in mid-year 1999 and continuing at an accelerated pace through May 2002, the company (under the direction of Ebbers, Scott Sullivan (CFO), David Myers (Comptroller) and Buford "Buddy" Yates (Director of General Accounting)) used fraudulent accounting methods to mask its declining earnings by painting a false picture of financial growth and profitability to prop up the price of WorldCom's stock.

The fraud was accomplished primarily in two ways: Under-reporting 'line costs' (inter connection expenses with other telecommunication companies) by capitalising these costs on the balance sheet rather than properly expensing them. Inflating revenues with bogus accounting entries from "corporate unallocated revenue accounts".

In 2002, a small team of internal auditors at WorldCom worked together, often at night and in secret, to investigate and unearth US\$3.8bio in fraud.¹⁴ Shortly thereafter, the company's audit committee and board of directors were notified of the fraud and acted swiftly: Sullivan was fired, Myers resigned, Arthur Andersen withdrew its audit opinion for 2001, and the US Securities and Exchange Commission (SEC) launched an investigation into these matters on 26 June 2002. By the end of 2003, it was estimated that the company's total assets had been inflated by around US\$11bio.

On 14 April 2003, WorldCom changed its name to MCI and moved its corporate headquarters from Clinton, Mississippi, to Dulles, Virginia. Under the bankruptcy reorganisation agreement, the company paid US\$750mio to the SEC in cash and stock in the new MCI, which was intended to be paid to wronged investors.

Company: WorldCom

Country: US
Key date: 2002 (WorldCom filed for bankruptcy)

Dennis Kozlowski

Dennis Kozlowski, was Tyco's CEO in 2002. Tyco manufactured a wide variety of products, from electronic components to healthcare products. The conglomerate operated in over a hundred countries around the world and employed 240,000 people.

Dennis Kozlowski together with Mark Swartz, Tyco's then CFO; and Mark Belnick, the company's chief legal officer, took over US\$170mio in loans from Tyco without receiving appropriate approval from Tyco's compensation committee and notifying shareholders.

For the most part these loans were taken with low to no interest. Many of them were offset as bonuses without open approval. Kozlowski and Swartz also sold seven and a half million shares of Tyco stock for US\$430mio again without telling investors. Formal charges were made by the SEC in September, 2002 and all were found guilty of securities fraud violations.

Perhaps the most eye catching of the allegations related to the abuse of corporate hospitality directed mostly towards senior employees of Tyco themselves.

Tyco has been able to regain much in lost ground under new leadership. Because the acts of securities fraud committed by former senior Tyco executives were concealed and, for the most part, disguised, the majority of Tyco's employees were innocent. As a precautionary act, however, Edward Breen, who replaced Kozlowski, removed nine members of Tyco's original board.

Company: Tyco

Country: US
Key date: 2002 (Former CEO of Tyco and others arrested on securities fraud violations)

Calisto Tanzi

Calisto Tanzi founded Parmalat in 1961 a maker of long-life milk, yogurts and juice and ran it until 2003. The company, which had annual sales of around €7.5bio (US\$9.2bio), was the largest Italian food company and the fourth largest in Europe, controlling 50% of the Italian market in milk and milk-derivative products. It had 36,000 employees and offices in 29 countries around the world. It was based in Parma, about 250 miles northwest of Rome. Parmalat grew to success as a family run enterprise and became one of the emblems of northern Italy's business prosperity.

The Company became engulfed in crises when a Bank

of America letter confirming Parmalat bank account credits of €3.9bio (\$4.9 billion) was revealed as a forgery and didn't exist and that €8mio in bonds of investors' money had evaporated as well.

Parmalat filed for bankruptcy in December 2003 after information emerged that a decade-long fraud had left the company saddled with €14bio (US\$18.57bio) in debt.

Prosecutors subsequently uncovered a global web of offshore companies and a myriad of documents that had been falsified often in crude ways, such as forged on a scanner and then run though fax machines to make them look authentic.

An Italian court sentenced Parmalat founder Calisto Tanzi to 18 years in prison for his role in the 2003 collapse of the Italian dairy firm, after a seven-year investigation and sometimes called "Europe's Enron". Parmalat was the largest bankruptcy in European history, representing 1.5% of Italian GNP, proportionally larger than the combined ratio of the Enron and WorldCom bankruptcies to the US GNP.

The court in Parma, the dairy firm's headquarters, ruled that Mr Tanzi, the company's former chief financial officer, Fausto Tonna, Mr Tanzi's brother Giovanni and several other executives were guilty of fraud that led to Parmalat's bankruptcy.

Messrs Tanzi and Tonna were also ordered to pay a combined €2bio to Parmalat, which since the bankruptcy has been restructured and relisted. The court also ordered those convicted to pay creditors 5% of the nominal value of the shares or bonds that they had bought in Parmalat.

The fraud went back 15 years and initiated to cover up industrial and financial losses, not to extract money from the company.

The problems at Parmalat can be traced back to a decision in 1997, when Parmalat decided to become a "global player" and started a campaign of international acquisitions, especially in North and South America, financed through debt. The firm also engaged in several exotic enterprises, such as a tourism agency called Parmatour, and the purchase of the local soccer club Parma. Huge sums were poured into these two enterprises.

The massive expansion, instead of bringing in profits, contributed significant losses.

While accumulating losses, and with debts to the banks, Parmalat started to build a network of offshore companies, which were used to conceal these losses. The Companies were made to appear as assets or as a net provider of liquidity to the Parmalat group. In order to finance the continuing losses, Parmalat issued bonds the security for which was provided by the alleged liquidity represented by the offshore schemes.

The Bond issues were arranged by Banks including Citigroup, Deutsche Bank and Morgan Stanley who were then charged but later acquitted of an administrative charge for failing to have adequate procedures in place to prevent the fraud that led to the collapse. The banks argued that they too were victims of Parmalat's fraud and committed no wrongdoing. The prosecutors had sought to confiscate €120mio from the banks in damages and penalties. BOA also charged had earlier reached a settlement with Parmalat paying US\$100mio. Two further Banks, UBS and Credit Suisse both agreed to settle civil cases relating to the issuance of Bonds paying a total of €184.1mio (US\$284.7mio) and €172.5mio (US\$266.8mio) respectively.

Nextra, the fund-management arm of Italy's Banca Intesa, agreed to pay €160mio (US\$197mio) to Parmalat. The sum represented its settlement of prospective charges that it bought and sold €300mio of Parmalat bonds in the months before the collapse, knowing that there was fraud at the company. Banca Intesa said that it wanted to avoid protracted litigation, but maintained that its dealings with Parmalat had been "absolutely correct".

Company: Parmalat

Country: Italy

Key date: 2003 (Parmalat, the Italian Dairy company filed for bankruptcy and would become known as Europe's Enron)

Helmut Elsner & Others

In July 2008, a Vienna court sentenced nine people to prison for their role in causing €1.7bio (US\$2.6bio) losses at the fourth largest Austrian bank, Bawag PSK. Bawag's former chief executive Helmut Elsner and eight other defendants received jail terms over failed speculative investments and the cover up of these losses through balance sheet fraud.

While Elsner's actions did not directly result with the failed trades causing the losses, he was considered as the mastermind behind the scandals in the cover up of the losses and as a consequence he was given the longest prison sentence of nine and a half years.

In a trial that involved numerous parties, and lasting

nearly a year, the final sentences imposed were more severe than expected, presumably setting a standard for the legal responsibility of bank executives and auditors. BAWAG, literally translating to 'the Bank for Employment and Commerce', has a very interesting history. Founded in 1922, with the intention of extending 'favourable terms of credit to ordinary people', the bank was known to have had close ties to the Social Democratic Party of Austria and Labour Unions. In 2004 The Austrian Trade Union Federation (ÖGB) became the sole owner of Bawag. However this history was soon tarnished with what was considered as one of the biggest financial scandals in Austria since World War II.

The 'Bawag scandal' or 'Bawag affair' became public following revelations of Bawag's involvement with a US brokerage firm, Refco, which faced bankruptcy in 2005.

In October 2005, Refco announced that Phillip Bennett (Refco's former Chief Executive and Chair) had hidden €281mio (US\$430mio) in bad debts from the company's auditors and investors and had agreed to take a leave of absence. Bennett had been involved in buying bad debts from Refco in order to prevent the company from needing to write them off and was in turn paying for the bad loans with money borrowed from Refco itself.

Bawag had provided a loan of €350mio to Bennett, just days before the brokerage firm filed for bankruptcy protection in October 2005. The bank had also extended a €75mio loan to Refco itself. A few days subsequent to the receipt of this loan, Bennett was arrested in the US and charged with falsifying Refco's books. The bankruptcy filing took place a week later. Bawag agreed to pay €441mio (US\$675mio) to avoid US prosecution, as they had been named as "co-conspirator" in the fraud which led to the demise of Refco. The US authorities stated that Bawag had assisted Refco in masking its bad debt, through the credit it had provided to Bennett. Bennett was sentenced to 16 years imprisonment by the US authorities in July 2008.

In the process of these investigations into Refco, details emerged of Bawag's suspicious accounts in relation to their investments in the Caribbean. The Austrian Financial Market Authority announced a special investigation into the credit line that Refco was given by Bawag. The involvement of Bawag in the Refco scandal was overshadowed by revelations that Bawag had tried to cover up years of losses they had themselves incurred.

Bawag's losses occurred as a result of a series of failed bets using risky derivative investments on off-balance-

sheet vehicles, from 1995 to 2000. These trades were undertaken by Wolfgang Floettl. Floettl was the son of former Bawag CEO, Walter Floettl, Elsner's predecessor.

When Elsner became a Chief Executive in 1995, he encouraged Floettl to make risky and highly speculative investments into currencies to boost Bawag's earnings. Floettl made investments which were unprofitable, mainly speculative trades in Yen derivatives, which led to severe losses as a result of a depreciating Yen in 1998. By October 1998, Floettl bet the entire fund available to him on the falling Yen, losing more than €392mio (US\$600mio) in days. Again in 1999 and 2000, Floettl bet two more tranches of Bawag's cash in currency deals, making a loss on both.

Elsner instructed other board members to conceal the losses incurred by Floettl which had reached approximately €1.6bio (US\$2.4bio) by the end of 2000. Senior management conspired to disguise the losses through manipulation of Bawag's accounts. At the end of 2000 it was decided by Bawag's senior management (Wenigner and Verzettlnich), that these losses would be kept hidden. Several smaller business branches of the ÖGB, including the so called ÖGB-Privatstiftung which covered the 'strike fund' were used as collateral to avoid a substantial one-off write-down. Wenigner and Verzettlnich argued that this was the only way of protecting the bank.

These concealments did not become public until investigations into Refco uncovered suspicious Bawag accounts. During the trial while Elsner claimed that Floettl ignored investment rules by opting for riskier products, Floettl in contrast insisted that he was allowed to invest in such a way. However, the sentencing reflected the firm stance the authorities took against the parties that played a key role in encouraging the speculative trades, through use of unauthorised funds, followed by a calculated cover-up of the losses.

Helmut Elsner was sentenced to nine-and-a-half year imprisonment by the Vienna District Court following a conviction of fraud; breach of trust and falsification of the balance sheet. In December 2010, the Austrian Supreme Court reduced the length of sentence given to Elsner by the Vienna District Court in July 2008, to seven-and-a-half years following an appeal.

The Supreme Court also partially overturned the lower courts verdict by quashing Elsner's conviction of charges of fraud and falsification of the balance sheet. The Court also ruled that Bawag had sustained losses of €1.2bio as a result of Elsner's actions, as compared with the lower court's estimate of €1.7bio.

In July 2011 Elsner was released from prison due to his fragile health condition, having spent a period of four and a half years in prison. Wolfgang Floettl fully co-operated with the investigations and was sentenced to two-and-a-half years in prison (with 20 months of his sentence suspended) for aiding breach of trust in a minor case.

Robert Reiter, a former KPMG partner, in July 2008, was sentenced to one year in jail and two years on probation for colluding in the cover-up. The verdict against Reiter was considered most surprising as there had been doubts over his culpability. Other defendants involved in the cover up of the losses included Wenigner and Verzettlnich. Verzettlnich was the only Trade Union representative made aware of the losses and played a part in hiding them. They received sentences ranging between two and five years, some with partial suspension. Bawag was protected from bankruptcy by declarations of support from the ÖGB, its shareholder. However, due to ÖGB's ownership, the 'Bawag Affair' of 2006, was considered to have had wider political consequences. In order to diffuse the negative political impact of these scandals, in December 2006, Bawag was sold to the US investment firm Cerberus Capital Management. This was seen as a necessary step to protect the Austrian financial community and Austria's international reputation.

Company: BAWAG

Country: Austria

Key date: 2008 (former CEO of Austrian Bank BAWAG, sentenced to imprisonment for fraud)

B Ramalinga Raju

B Ramalinga Raju created India's fourth largest IT outsourcing company, Satyam Computers Services ("Satyam"), and was regarded as a leader and inspiration by the 50,000 strong work force of Satyam and numerous industry observers, customers and stakeholders.

Under Raju's helmsmanship Satyam boasted of 185 Fortune 500 companies as customers and operations in 66 countries. Satyam had also won two Golden Peacock awards for Excellence in Corporate Governance in 2002 and 2008 respectively and Raju himself was awarded with the Entrepreneur of the Year Award in 2007 by Ernst & Young. Raju maintained that company's staunch commitment to training and educating its people and understanding its customers had worked in its favour.

Satyam was consistently rated among the best employers in India and had the highest employee cost to sales ratio of around 60% compared to 50-53% reported by its larger peers.

Raju, who hails from a wealthy agrarian family from Andhra Pradesh, one of the southern states in India, holds a Bachelor of Commerce (B.Com) Degree and a Masters in Business Administration (MBA) from Ohio State University. He initially ventured into textiles and real estate businesses but found his forte in IT with Satyam which he started in 1987 with only 20 employees and later took public in 1992 in a high profile IPO which was oversubscribed 17 times.

For the intensely competitive and ambitious Raju who wanted to be ahead of his peers and competitors and had staked claim to being the fastest growing IT company in India, troubles apparently began when he announced Satyam's plans on 16 December 2008 to enter the depressed realty and infrastructure sector by buying all of privately held Maytas Properties for US\$1.3bio and 51% of builder Maytas Infra for US\$300mio, as he thought it would "de-risk" Satyam's core business in IT services. The two companies were promoted by Raju's family, Satyam's promoters owned 35% stake in Maytas Properties and 36% in Maytas Infra and Raju's sons sat on the boards.

By trying to enter into related-party deals without shareholder approval, Satyam lost investors' trust. Satyam's stock came under severe pressure after the announcement and institutional investors showed their displeasure by hammering the stock both on the NYSE and National Stock Exchange causing the stock to drop by 55% and 33% respectively.

Raju was forced to call off the deal but in the process the market capitalisation of Satyam fell by US\$1bio to US\$2.23bio on 17 December from US\$3.2bio. His troubles compounded with the World Bank barring Satyam from doing any business with it for the next eight years upon allegations of "malpractice's including bribery" on 24 December 2008. News reports indicated that the World Bank debarment, the harshest sanction ever made by the bank since 2004, was meted out for 'improper benefit to bank staff' and 'lack of documentation on invoices'. Resignation by four independent directors on the board of Satyam followed quickly. While Satyam's stock took a beating on the stock exchanges, the company's image took a drubbing by the national and international media.

Just over a week later, on 7 January 2009, Raju released a letter addressed to the Board of Directors of Satyam with copies to the chairman of the Securities and Exchange Board of India and the stock exchanges where Satyam's stock was listed which would bring to light the biggest fraud in corporate India.

In the letter, Raju revealed shocking facts – that he had falsified the accounts of Satyam such that the reported financials of Satyam now had a gap of US\$1.2bio from the actual. He claimed that Satyam's balance sheet carried very large inflated/non-existent cash and bank balances, accrued interest and debtors

and understated liabilities. Raju further stated that the revenue for September quarter alone were overstated by approximately US\$131mio and operating margin by US\$117mio.

Raju stated in the letter that what started as a marginal gap between actual operating profit and the one reflected in the books of accounts continued to grow over the years. The differential in the real profits and the one reflected in the books was further accentuated by the fact that the company had to carry additional resources and assets to justify higher level of operations -thereby significantly increasing the costs.

Raju averred that every attempt made to eliminate the gap failed and as the promoters held a small percentage of equity, he was concerned that poor performance would result in a take-over, thereby exposing the gap. He compared it to "riding a tiger, not knowing how to get off without being eaten."¹⁵

Raju claimed in the letter that in the past two years a net amount of US\$246mio was arranged to Satyam to keep the operations going by resorting to pledging all the promoter shares and raising funds from known sources by giving all kinds of assurances. These loans and transactions were not reflected in the books of Satyam either. However as the value of Satyam's stock fell, most of the pledged shares were sold by the lenders on account of margin triggers. This was the last straw for the once-dominant entrepreneur who found himself irretrievably tangled in the complex web of financial chicanery he had woven and led to his confession.

He revealed that the aborted Maytas acquisition deal was the last attempt to fill the fictitious assets with real ones. Maytas' investors were convinced that this was a good divestment opportunity and a strategic fit. Raju believed that once Satyam's problems were solved, given the family ownership of Maytas, its payments could be delayed. However, that stratagem failed due to the adverse reaction of investors. Further, perversely, the market reaction to the news and the resulting fall in Satyam's stock further escalated the situation.

The revelation sent shock-waves through the stock markets with NYSE halting trading in Satyam's stocks. The NSE removed it from its key indicator index.

On 10 January 2009 the Company Law Board decided to bar the current board of Satyam from functioning and appointed 10 nominal directors. Raju was arrested followed by the arrest of Satyam's then-CFO on 11 January 2009. The Government appointed several eminent individuals to the board of Satyam and lent its support to the troubled IT giant in order to save jobs and confidence in corporate India.

Two Pricewaterhouse partners responsible for the audit of Satyam's financials were also arrested, charged with criminal conspiracy and falsification of accounts. Pricewaterhouse also announced the resignation of its assurance leader in India. (An assurance leader oversees a firm's audit practices, policies and procedures, and growth and quality control.) PWC has also been charged in at least one class action suit in the US in relation to Satyam by the ADR holders for having 'recklessly disregarded' a multi-year massive fraud by the former management of Satyam.

Several investigative, enforcement and regulatory agencies swung into action to investigate the fraud and pin responsibilities, including the Crime Investigation Department, Serious Fraud Investigation Office and SEBI.

The chargesheet presented by the prosecutor alleged that Raju forged Satyam's fixed deposits documents, diverted as much as US\$4mio monthly from the IT company, held more than 400 land transactions running into thousands of acres under shadow names, and claimed that the company overstated employee numbers by 13,000. Raju was personally charged with several offences, including criminal conspiracy, breach of trust, and forgery and still languishes in prison without bail while the case against him makes its way through the court processes. Satyam has been sold through an open bidding process overseen by the Government-appointed board of directors to Mahindra & Mahindra.

Tech Mahindra, the IT arm of Mahindra and Mahindra, an Indian conglomerate, bought a majority stake in Satyam (now renamed Mahindra Satyam) at approx. US\$1.23 per share. Given Satyam had touched, and traded at, a high of approx US\$12, this was a mere 10% of the value of Satyam shares at their peak. Tech Mahindra paid a total consideration of US\$646mio.

The Satyam case raised several questions about effectiveness of corporate governance in Indian companies and led to action by Companies Law Board, SEBI and other authorities for stronger corporate governance.

The case also brought into focus the risks of continued family-control over listed companies, particularly by founders. Some of the outcomes of the shocking Satyam scandal are strengthening the role of non executive/independent directors, greater accountability of statutory auditors and tightening of disclosure norms around stocks held by promoters including disclosure of pledging of stock. Interestingly, there were no additional red-flags in terms of numbers or financials. Satyam had

slightly higher than industry norm employee cost ratio and lower net operating margins, however nothing alarming. They were known to be aggressive in acquiring business and under-cutting peers on price. They showed a healthy cash & equivalent balance of over US\$1bio which tied in with other cash-rich IT players. Perhaps the only cause of concern was the tight control maintained by the Raju family in running the company though there were professional managers appointed to take care of the company's affairs. The reason the scam sustained for the period it did was due to the complicity of the CFO with Raju in falsifying books and accounts and the failure on the part of the auditors to verify documents/check for fraud.

Company: Satyam
Country: India

Key date: 2009 (Raju writes a letter exposing massive fraud at his Indian Company Satyam)

Tsuyoshi Kikukawa and Others

In February 2012, Seven Olympus executives were arrested by Japanese police and prosecutors. Olympus Corporation is a major Japanese manufacturer of camera's lenses and similar and/or related optics and reprography products. Ex-president Tsuyoshi Kikukawa, former executive vice president Hisashi Mori and former auditor Hideo Yamada were taken into custody on suspicion of violating the Financial Instruments and Exchange Law, along with former bankers Akio Nakagawa and Nobumasa Yokoo and two others, suspected of having helped the board hide significant losses. On 25 September 2012, the company and Kikukawa, Yamada and Mori pleaded guilty to collusion to submit false financial reports.

The charges spring from events in late 2011, when the company fired its newly appointed British CEO Michael Woodford, following his concern and notification about very dubious company activities precipitating a scandal that wiped 75% off the company's stock market valuation. Woodford alleged that his removal was linked to several prior acquisitions he questioned, particularly the US\$2.2bio deal in 2008 to acquire British medical equipment maker Gyrus Group, where it has been reported that US\$687mio was paid to a middle-man as a success fee, a sum equal to 31% of the purchase price and that the company acquired three other Japanese companies outside its core business and recognised that the assets were worth US\$721mio less than their acquisition value 12 months previously.

Following his dismissal, Woodford passed on information to the British Serious Fraud Office, and

requested police protection. He said the payments may have been linked to "forces behind" the Olympus board. Japanese newspaper Sankei suggest that a total of US\$1.5bio in acquisition-related advisory payments could be linked to the Yakuza. In June 2012, Olympus announced it would cut 2,700 jobs, or 7% of its global work force, by the end of March 2014 and will scrap around 40% of its 30 manufacturing plants around the world by the end of March 2015 to reduce cost due to investment losses of Yen117.7bio (US\$1.5bio) dating back to the 1990s.

Company: Olympus

Country: Japan

Key date: 2012 (Arrests of top management)

Advanced Fee Fraudsters

Special Focus 10 Chief Nwude & Banco Noroeste



Banco Noroeste was a Brazilian bank at the centre of a Nigerian 419 scam, which was described as the "single biggest advanced fee fraud case in the whole world" by the former chairman of Nigeria's Economic and Financial Crimes Commission (EFCC), Alhaji Nuhu Ribadu. The

draining of approximately US\$242mio from the Brazilian Bank Noroeste was discovered in 1998 after its sale to the Spanish group Santander.

The branch of the bank in Cayman managed the Capital of the Bank holding blue chip investments in US banks such as JP Morgan and Bank of New York. Between May 1995 and February 1998, a total of US\$242mio was reportedly stolen from the Banco Noroeste S. A. through offshore banks in the Cayman Islands.

Whilst the fraud appears to have been a 419 Advance Fee Fraud scam, there are also suggestions that whilst it may have started this way, a senior employee of the Bank may have been involved also.

The senior employee in question was Nelson Sakaguchi, Head of Noroeste's Cayman Branch, who on a business trip to Nigeria in 1994, was introduced to Chief Nwude who purported to be Paul Ogunwuma the Governor of

the Central Bank of Nigeria. Sakaguchi was asked to invest in a proposal to build a new Airport in Abuja, promising big returns. Despite his experience, Sakaguchi agreed and gave the instructions to liquidate the Cayman Branch's blue chip investments and to invest US\$190mio in the fake project.

Following the discoveries, Chief Nwude and his associates were charged in Nigeria and convicted of obtaining US\$190mio by false pretences. They pleaded guilty and forfeited US\$170mio in assets.

Penalty: convicted of fraud

Actions: longest advance fee fraud recorded

Country: Nigeria, Brazil, Cayman Islands

Key date: 1998 (Nwude charged with masterminding the largest advance fee fraud in history)

Hasan Ali Khan

Hasan Ali Khan or Syed Mohammed Hasan Ali Khan is currently charged in India with money laundering on a massive scale.

According to the Indian authorities, the 56-year-old scrap metal dealer and stud farm owner has over US\$8bio in assets which if true would make him one of the richest men in India. In early 2007 the Indian authorities raided Mr Khan's Pune residence and came across documents that purportedly showed that he had billions of dollars in accounts at UBS in Switzerland with possibly additional funds in other accounts in other banks. Such alleged wealth seems totally contrary to both the known business activity of Mr Khan and his more modest lifestyle.

The document that has received most attention from the raid was a letter purportedly from UBS in Zurich, dated 2006 and written "to whom it may concern" with the subject heading stating Hasan Ali Khan.

The letter, available on the internet, read as follows - Khan can withdraw US\$6bio was free to invest this amount as and when he chooses to do so and that the balance amount of US\$2.04bio would remain bound with UBS until 15 January 2007, after which Khan was free to invest the same as and when he chooses to do so." The letter was on UBS Ltd letterhead and was allegedly signed by the then CEO.

Further claims according to charges brought against Khan are that Khan dealt with the notorious Saudi arms dealer from the 1970s, Adnan Khashoggi in a US\$300mio missile deal through UBS and that Khan when negotiating to pay approx CHF28mio for a Swiss Chateau that UBS had confirmed that these monies could be paid from Khan's "petty cash".

UBS both in 2007 and since, repeated and issued press releases stating that the document is a crude forgery and its contents are untrue.

The case has generated massive media interest in India and even the attention of the Indian Supreme Court which has personally intervened in the case amid concern that the Indian authorities have failed to fully investigate the case or are failing to pursue the case thoroughly. This concern is heightened as the case has been linked with allegations that Mr Khan may have acted for and/or be fronting for leading Indian politicians in moving and hiding massive monies amassed from corrupt activities in India and that the investigation is being hampered by and Mr Khan somehow being protected by political interference.

Country: India

Key date: 2007 (Khan arrested in India)

Hedge Fund/Investment Co Fraudsters

Jordan Belfort

Jordan Belfort was convicted of fraud related to stock market manipulation and running a penny stock boiler room for which he spent 22 months in prison. His story has been made into the recent movie, "The Wolf of Wall Street", released in 2013, starring Leonardo DiCaprio but also the movie "Boiler Room", released in 2000 and starring Ben Affleck, was inspired by Belfort's operation. Belfort was born in New York to Jewish parents, one an accountant and one a lawyer. He started his financial career as a broker at L.F. Rothschild, before starting his own brokerage firm Stratton Oakmont in the 1980s with partner Danny Porush.

Belfort never ran a legal operation, his intent was to establish a boiler room operation marketing penny stocks, where he defrauded investors with fraudulent stock sales, underrating classic pump and dump manipulation techniques. For example, Belfort and several of his executives would buy up a particular company's stock and then have an army of brokers (following a script he had prepared) pump it up by selling it to unsuspecting investors. This would cause the stock to rise, pretty much guaranteeing Belfort and his associates a substantial profit, who would then dump the stock or sell out. Soon after the stock would fall back to reality, with the investors bearing a significant loss, effectively Belfort defrauding the investors and taking much of their money.

At its peak in the 1990s, Stratton Oakmont, Belfort's firm that he co-founded with Danny Porush, employed more than 1,000 brokers. During his years at Stratton Oakmont, Belfort developed a lavish partying lifestyle,

which included a serious addiction to drugs. In 1996 Stratton Oakmont was banned from the brokerage industry, which eventually forced the company to close its doors.

Belfort was indicted in 1998 for securities fraud and money laundering. After cooperating with the FBI, he served 22 months in prison admitting responsibility for approximately US\$200mio in investor losses. Belfort was ordered to pay back US\$110mio. Danny Porush served 39 months in prison for his part in the fraudulent dealings of Stratton Oakmont.

Country: US

Key Date: 1996 (Stratton Oakmont, Belfort's firm was closed down)

Michael Brown

A brash, ponytailed Michael Brown from Glasgow, UK, claimed to be a successful offshore trader living in Majorca, whose clients included, Martin Edwards, the former Manchester United Chairman, who had invested £8mio with Browns company, 5th Avenue Partners. Instead of investing this and other client funds, Brown used the money for his own purposes, and after his arrest on fraud charges in the UK he disappeared from Britain while on parole and was sentenced in his absence to seven years in prison. Whilst he would later be found and arrested in the Dominican Republic, it was how he used some of the money that brought him to the attention of the UK media. As the UK elections approached, Brown met in 2004 with the UK's third largest Party, the Liberal Democrats, bankrolling the party with £2.4mio of stolen money and becoming their biggest ever donor. Within months, Brown was flying Lib Dem leader, Charles Kennedy across Britain in a private jet and was being invited to dinners in Mayfair.

Despite not being a party member, not being registered to vote and living abroad, he was welcomed with open arms by the Lib Dems who clearly failed to conduct proper due diligence. Despite the fact that the funds were the proceeds of a crime, and notwithstanding the fact that the Lib Dems failed to conduct adequate due diligence, the Lib Dems maintain that the money was received in good faith and refuse to return the funds. Due diligence rules on campaign finance monies differ from those applying to financial institutions accepting monies from customers markedly. In the UK and elsewhere, Political Parties are restricted from receiving donations from foreign persons so as to prevent foreign involvement in a third country's politics. In this case whilst monies were received directly from a foreign company, namely, 5th Avenue Partners, this was the investment vehicle controlled by the British citizen,

Michael Brown. Therefore, whilst a technical violation may have occurred, Brown was entitled to fund the Lib Dems and they were entitled to accept his donation. What is less palatable is that as this was the largest ever donation made to the Lib Dems, from a source that was not known to them, it was essentially a walk-in supporter without any history of previous support, without adequate care and attention being sought as to his source of funds and the fact that he turned out to be a fraudster, enough red flags should have caused the Lib Dems to reject the donation. Instead not only did they accept and spend the funds, but then once the facts had been established they refused to return the funds and to claim in their defence that the parliamentary investigation had exonerated them, when in fact it had simply confirmed that as Michael Brown was a UK citizen they had not broken that part of UK finance rules, nothing more.

Country: UK
Key date: (charged in UK on fraud charges after donating criminal proceeds to UK political party)

Samuel Israel III

The most common form of reported fraud involving hedge funds relates to offences perpetrated by hedge fund managers against their customers, especially in terms of false or misleading net asset valuations. Exaggerated statements of assets under management and net annual profits are not unknown in the hedge fund world. From 1996 until 2005, Samuel Israel III managed a group of US onshore and Cayman Islands offshore hedge funds under the family name Bayou (the "Bayou funds"). While these hedge funds were apparently originally conceived as legitimate investment vehicles, large trading losses during early fund operations forced the managers to conceal the losses through a variety of false accounting practices, including issuing false financial statements to investors and fabricating false "independent audit reports" by creating a sham accounting firm.

In April 2004, the fund managers in an attempt to win back losses incurred suspended trading on behalf of the funds, emptied their prime brokerage accounts, and wire transferred US\$150mio into Citibank's Bayou account. Of this US\$150mio, they moved US\$120mio into a German bank account in the name of one of the fund managers for investment in a "prime bank instrument trading programme". They had been convinced by a third fraudster that massive returns were possible investing in these secretive prime bank instruments. With the Banks suspicious, Israel was warned that he might be being defrauded though he didn't take their warnings seriously. Ultimately the

third fraudsters didn't get the remaining Bayou funds but the original Fraud was uncovered when large value, third party international wire transfers, coupled with other third party fund movements, lack of apparent legitimate business activity and large dollar values of the account, caused the retail bank involved to contact the authorities, who ordered the funds to be frozen, prosecuted the fund managers.¹⁶

Country: US, Cayman Islands
Key date: 2005 (Fund Managers arrested and prosecuted for Fraud)

Special Focus 11 Bernie Madoff



Bernie Madoff orchestrated the largest Ponzi scheme ever recorded. In December 2008, he was charged in both a criminal information and US Securities and Exchange Commission (SEC) complaint alleging that he ran a multi-billion dollar

Ponzi scheme. Madoff settled the SEC suit and on 12 March 2009, he pleaded guilty to the criminal information that charged him with security fraud resulting in investor losses of US\$10-17bio. The information largely contained Madoff's admissions of his criminal conduct he made to his two sons shortly before his arrest. His plea ended the criminal matter, and the full details of his scheme were thus never detailed in an indictment. At his pleading allocution, however, Madoff admitted to running a Ponzi scheme that he stated began in the early 1990s. He acknowledged that he did not invest any of his clients' money, but rather deposited the money into his business account at JP Morgan Chase & Co (JPM). To conceal the scheme, he admitted to false trading activities masked by foreign transfers and false SEC returns. When clients requested account withdrawals, he paid them from the JPM account, claiming the profits were the result of his own unique "split-strike conversion strategy". On 29 June 2009, Federal District Judge Denny Chin sentenced Madoff to the maximum sentence of 150 years in prison.

The Madoff case has resulted in a proliferation of books and other media accountings of his decades-long scheme, as well as US Congressional hearings and

regulatory reforms. At its core, Madoff perpetrated a classic Ponzi scheme by paying investors with other investor funds. What separates Madoff from other Ponzi schemes is the sheer breadth in terms of: the dollars; the investors (individuals to large institutional victims); the global reach of his investors and feeder funds; and duration (decades). Moreover while most Ponzi and Investment Fraud schemes rely on the promise of high returns for investments in unregistered instruments or unconventional investment strategies, Madoff's scheme involved false trading returns through a regulated broker-dealer. In the aftermath, much of the public attention as to why this scheme went undetected focused on the shortcomings and failures of the regulators, primarily the SEC, but like any other Ponzi scheme, Madoff needed the use of a financial institution to gather and move the cash. Questions of AML controls by the financial institutions that did business with Madoff have largely been raised in civil actions brought by the Trustee appointed for Madoff's Broker Dealer in his efforts to recoup funds for the victims of the scheme and by the US authorities, for example, against JP Morgan for failures on their part which have resulted in fines of US\$2bio being incurred.

Madoff was a former Chairman of the board of directors of the NASDAQ stock market.

In the early 1960s, he founded Bernard L. Madoff Investment Securities LLC, (BMIS) a registered Broker-Dealer and Investment Advisory Firm. The Firm had three distinct business lines - investment advisory services, market making services, and proprietary trading. The Ponzi scheme was conducted through the advisory services arm in which Madoff falsely reported investment earnings to his clients when in fact no trades were ever executed. In fact, in classic Ponzi scheme formula, he reported consistently high returns on investments through fictitious trades and when investors sought to redeem their investments, Madoff simply paid investors with funds he obtained from other investors. The scheme collapsed during the 2008 credit crisis when Madoff could not keep up with finding new investor funds to match the redemption demands. Given the enormity of the fraud, few believed Madoff's claims that he acted alone. Criminal cases have since been brought against BMIS back office employees, and criminal pleas have been entered by Frank DiPascali, Jr., the CFO and Director of Operations Trading at BMIS, and David Friehling, BMIS' CPA.

In addition to the Congressional Hearings, in August 2009, the SEC's Office of Investigations (OIG) issued its report, Investigation of Failure of the SEC to Uncover Bernard Madoff's Ponzi Scheme.¹⁷ The report

detailed failures of the SEC to uncover the scheme, and found that: "the SEC received more than ample information in the form of detailed and substantive complaints over the years to warrant a thorough and comprehensive examination and/or investigation of Bernard Madoff and BMIS for operating a Ponzi scheme, and that despite three examinations and two investigations being conducted, a thorough and competent investigation or examination was never performed ...". The OIG also found that numerous private entities conducted basic due diligence of Madoff's operations and, without regulatory authority to compel information, came to the conclusion that an investment with Madoff was unwise. Specifically, Madoff's description of both his equity and options trading practices immediately led to suspicions about Madoff's operations. With respect to his purported trading strategy, many simply did not believe that it was possible for Madoff to achieve his returns using a strategy described by some industry leaders as common and unsophisticated ... The private entities' conclusions were drawn from the same "red flags" in Madoff's operations that the SEC considered in its examinations and investigations, but ultimately dismissed."

Before Harry Markopolos first raised his concerns to the SEC in 2000 that went unheeded, the OIG also found that the SEC missed an opportunity to detect Madoff's Ponzi scheme from their review in the early 1990s into claims made by investors of a Ponzi scheme regarding the investment firm, Avellino & Bienes.

The OIG report noted that the: "The SEC was provided with several documents that Avellino & Bienes created that indicated that they were offering "100%" safe investments, which they characterized as loans, with high and extremely consistent rates of return over significant periods of time. Not everyone could invest with Avellino & Bienes, as this was a "special" and exclusive club, with some special investors getting higher returns than others. As the SEC began investigating the matter, they learned that Madoff had complete control over all of Avellino & Bienes' customer funds and made all investment decisions for them, and, according to Avellino, Madoff had achieved these consistent returns for them for numerous years without a single loss. Avellino described Madoff's strategy for these extraordinarily consistent returns as very basic: investing in long-term Fortune 500 securities, with hedges of the Standard & Poor's (S&P) index. The SEC suspected that Avellino & Bienes was operating a Ponzi scheme and took action to ensure that all of Avellino & Bienes' investors were refunded their investments. Yet, the OIG found that the SEC never considered the possibility that Madoff could have taken the money that was used

to pay back Avellino & Bienes' customers from other clients as part of a larger Ponzi scheme."

Madoff's fraud, like any Ponzi scheme, involved the movement of funds to carry out its uniform objectives – steal from its investors and use the funds from other investors to conceal the fraud. The Madoff story has not been completely told as to whether institutions where he banked will be deemed, either civilly or from a regulatory perspective, to have had inadequate AML controls (JP Morgan have since admitted liability to mistakes and have been fined US\$2bio). The AML issues have largely been raised in the lawsuits filed by Irving Picard, the Trustee appointed for the Liquidation of Bernard L. Madoff Investment Securities LLC. Picard initiated civil proceedings against JPM, Madoff's primary banker, seeking US\$19bio in damages. The civil suit alleges JPM "was at the very centre of the fraud, and thoroughly complicit in it." To support this claim, the Trustee's complaint alleged certain notable red flags that its AML programme was "not effectively executed", including: - billions of dollars flowed through the BMIS account and no trading/investment activity ever occurred that would be consistent with either business purpose of the account – market making or advisory services; - the transactions were repetitive, in large dollar amounts and in certain situations, the same amount was sent in multiples to the same client on the same date; - many transactions involved hand-written cheques; - wire activity also involved the use of high risk offshore entities; -large amounts of funds were received from investors and funds sent out to other investors; - it noted that JPM was made aware back in 1997 that a financial institution on the other side of JPM transactions had concluded that the circular flow of funds between two Madoff accounts was suspicious and closed its business with Madoff; - since JPM maintained accounts for both BMIS and private bank accounts for two of its largest investors, it had greater visibility into the suspect transactions; and -despite the large fund movements, the circular transactions, no monitoring alerts were generated.

In addition, the complaint also alleged there were further red flags unrelated to transactional activity that JPM learned through its own due diligence from the structured product business it also conducted with certain Madoff feeder funds, such as: -BMIS' returns were consistently high even in down markets; -Madoff would not allow transparency into his trading strategy, nor would the feeder funds provide its trading agreements it had with BMIS to JPM in connection with its due diligence reviews of these funds; - Madoff would not reveal and the feeder funds had no idea of whom the purported counterparties were on his OTC

trading; -Madoff and BMIS had a conflict of interest since it acted as the clearing broker, sub-custodian, and sub-investment advisor; - concerns about the use of a small, unknown auditor for such a large business operation; and - JPM was in possession of certain regulatory reports that should have put them on notice that said filings were false since they maintained the banking relationship for BMIS.

Picard and investors have also filed law suits against financial institutions that serviced the Madoff-related feeder funds. The central theme to the theory of liability is that the institutions breached their fiduciary duties by failing to conduct adequate due diligence on Madoff and his funds before accepting millions of dollars.

Penalty: sentenced to 150 years imprisonment
Actions: affinity fraud and Ponzi scheme racking up US\$10-17bio in losses for investors
Country: US
Key date: 2008 (Madoff charged with operating the largest Ponzi scheme in history)

Sammy Goldman & Harry Tanner Jr

Florida based precious metals firm, American Precious Metals, LLC (APM) and its founders and principals, Sammy J Goldman and Harry Robert Tanner, Jr. offered customers the opportunity to make a lot of money, with little risk, by purchasing precious metals through a financing agreement, leveraging their investment and increasing their likely returns. Customers were asked to send a down payment, which came to as little as US\$5,000. APM would then finance up to 80% of customers' purchases and store customers' physical metals in a secure depository. In fact using this sales pitch APM should have purchased more than US\$23mio of precious metals for customers.

The reality was that this was a fraud. APM should have been regulated by the US Commodity Futures Trading Commission (CFTC) but it wasn't. It deducted 40% of all monies received as commissions, pooled the remaining funds and sent much of that money to a related third party. These monies were never used to buy precious metals or to provide storage. In May 2011 the CFTC prosecuted APM for this fraud. The CFTC then put out advisories to be alert to companies that sell investments in precious metals based on sales pitches claiming that customers can make a lot of money, with little risk, by purchasing metal through a financing agreement.

Country: US
Key date: 2011 (US CFTC prosecuted Goldman and

others for fraud)

Ponzi - Pyramid Schemes

Special Focus 12 Charles Ponzi



With less than three dollars in his pocket, Charles Ponzi emigrated from Italy to the US in 1903. In less than 20 years after his arrival, Ponzi was deported back to Italy and labeled as one of the most infamous fraudsters for orchestrating one of the biggest financial crimes of the 20th century.

Ponzi was constantly looking for ways to make his first million and at the end of 1918 he thought he had found a way. Ponzi's idea involved buying international postal reply coupons in European currencies at fixed, outdated rates of exchange and then redeeming them in the US for dollars. Ponzi saw an incredible opportunity since the currencies of post-World War I countries were in shatters and redeeming the postal reply coupons in the US almost guaranteed a profit. However, once Ponzi put his idea in motion he found that redeeming the coupons, at the volume he desired, was nearly impossible due to excessive postal regulations. Still determined, Ponzi started to tell friends and family that the returns available from postal reply coupons made impossible profits possible. Within weeks, immigrants swayed by Ponzi's investment venture proposal were transferring large sums of money to Ponzi with some receiving a 75% return. But what they didn't know was that Ponzi was paying investors who wanted to cash out with monies from newer investors or with monies from investors who were willing to reinvest with Ponzi. Unbeknownst to the investors of Ponzi's scheme, they further perpetrated the fraud by spreading the word of the returns he was able to achieve and an avalanche of investor funds ensued. To promote his investment venture further, Ponzi started a company and employed a multitude of agents to take in money from investors across the northeast coast. With money pouring in and investors choosing to reinvest rather than taking the profits, Ponzi began depositing the funds into Hanover Trust Bank of Boston with the goal of buying a controlling interest in the bank. It took Ponzi less than six months from his initial idea of investing in postal

reply coupons to buying a controlling interest in a small bank. Obviously his success raised suspicions, most notably by the press.

The Boston Post contacted the publisher of Barron's, a financial paper, to investigate Ponzi's investment company. Barron's investigation found that Ponzi did not invest in his own company and more troubling was the fact that 160 million postal reply coupons would have had to be in circulation to cover the investment Ponzi was claiming. The US Postal Service confirmed that no such quantity was in circulation; rather, there were around 27,000. Ponzi, aware of Barron's investigation, hired a publicist, William McMasters to counter the negative press. But after McMasters discovered documentation that Ponzi was an actual fraud, he went to the Boston Post to write a story of his findings. The cascade of negative press left Ponzi scrambling to pay out investors who were requesting their investments be paid back. The Massachusetts bank commissioner noticed the massive runs on Ponzi's investment company and an order was made in 1920 for bank examiners to watch Ponzi's accounts. A week after the order, examiners found there were enough investors who had cashed their cheques with Ponzi's main account that it was almost certainty overdrawn. After this discovery, the commissioner ordered Hanover Trust Bank not to pay out any more cheques from Ponzi's main account. This action forced the Massachusetts Attorney General to release a statement that there was little evidence to support Ponzi's claims of large scale dealing in postal reply coupons. Charles Ponzi's house of cards had fallen to the ground.

A day after the Attorney General released his statement Ponzi decided to turn himself in to authorities. He was charged with 86 counts of mail fraud but pleaded guilty to only one count and was sentenced to five years in a federal prison. After serving three and a half years, Ponzi was released and then immediately indicted on 22 counts of larceny by the State of Massachusetts and was sentenced to nine years in state prison. After only three years, he was released on bail and fled to Florida where he began another scheme, similar to his previous one, but this time relating to real-estate. Early in 1926, Ponzi was arrested and charged with violating Florida trust and securities laws. A jury found him guilty and he was sentenced to one year in prison. Before he served his time, Ponzi appealed his conviction and was freed after posting bond. Tired of running from the law and after failing at multiple schemes, Ponzi tried to flee back to Italy by jumping on a merchant ship, but was caught by the ship's captain and sent back to Massachusetts to serve the rest of his state prison sentence. He was released in 1934 and then deported to Italy as an

undesirable alien. At a charity hospital in Rio de Janeiro on 18 January 1949, Charles Ponzi died from health complications without a penny to his name.

To this day the name 'Ponzi' remains synonymous with large scale investment fraud and in particular pyramid schemes. A pyramid scheme is a form of fraud similar in many ways to a Ponzi scheme, relying as it does on the hope of an extremely high rate of return. One of the main differences of the two schemes is that Ponzi schemes are structured such that they use the entry fees from participants to make profits for the earlier entrants to the scheme; whereas a pyramid scheme usually requires that participants make a payment for the right to recruit additional participants, at which point they will receive money. A pyramid scheme is bound to collapse much faster because it requires exponential increases in participants to sustain it. By contrast, Ponzi schemes can survive simply by persuading most existing participants to "reinvest" their money, with a relatively small number of new participants. Unfortunately, investors still fall victim to this scheme even today because, among other reasons, they are lured by access to great wealth and exclusivity proffered by Ponzi's emulators.

Penalty: imprisoned many times for frauds
Actions: put his name to "Ponzi Schemes"
Country: US
Key date: 1920 (Ponzi scheme collapsed)

Special Focus 13 Ivar Kreuger



Ivar Kreuger was known as the "Match King" producing 75% of the world's matches in 1930. One biographer called him a "genius and swindler", John Kenneth Galbraith wrote he was the "Leonardo of larcenists. A national hero

in his native Sweden, Kreuger was admired for his generosity, including the loans he made to a dozen struggling countries. But after his suicide in 1932, the world learned about the true basis of his company.¹⁸ His father owned a small match factory, which he took over in 1917. Just a few years earlier, a Swedish professor had invented the safety match, a form of non-toxic phosphorous that could be manufactured on a box of matches. Seeing an opportunity for growth in post-war

Europe, he snapped up dozens of small match factories. He began approaching cash strapped countries with an attractive offer: he would make a sizable loan in exchange for a national monopoly on match production. The more matches he sold, the more money the government made in taxes. Whether because of desperation or Kreuger's skills of persuasion, a dozen countries signed up for the deal by 1930. Germany secured the biggest loan of US\$125mio.

Kreuger, who cultivated an image as a person more concerned about creating global stability than profit, loaned out approximately US\$253mio taking in monies from investors lured by the prospect of significant profits and dividends. Unable to pay the high dividends he promised, Kreuger turned his business into a Ponzi-Pyramid-type Scheme. On 12 March 1932, Kreuger committed suicide in a hotel room in Paris. At first, his death was deemed a "suicide while despondent." But, as the depth of the fraud was revealed, ill health was ruled out as a cause. With more new revelations, about other frauds in his business empire a so-called "Kreuger crash" ensued. Beyond the shock of seeing its national hero exposed as a criminal, Sweden sustained losses of about \$60 million. To stave off a complete meltdown, the government acted fast to put the equivalent of \$7 million into banks affected by the crash. In the US, legislation was drafted to fill in the gaps of oversight that Kreuger exploited. America's Securities Act, which passed in 1933, required greater disclosure on the part of companies seeking to sell stock.

Penalty: Suicide, loss of business empire
Actions: Fraud, giant Ponzi type scheme
Country: Sweden and elsewhere
Key date: 1932 (unavailing of major fraud)

Barry Minkow

Barry Minkow ran a carpet cleaning business in the US, starting as a 16 year old, establishing "ZZZZ Best" and growing it to a company with over 1400 employees who specialized in insurance restoration cleaning. The company went public in 1996 and temporarily had a market value of over US\$200 million. However, the company was simply a massive Ponzi scheme, raising money from new investors to pay off old ones, with thousands of documents forged to maintain the appearance of a thriving business.

The company quickly collapsed and Minkow and 11 others were indicted on 54 different counts of fraud. Minkow was sentenced to 25 years in prison, but served 7 1/2.

Country: US

Key date: 1986 (Company listed)

Rogue Traders

Special Focus 14 Nick Leeson



On 17 January 1995 a massive earthquake shook the Japanese city of Kobe damaging property and taking 6,434 lives. The shockwaves that took their toll on Kobe would also claim another victim, the oldest of British Banks, Barings Bank, which unbeknown to its senior

management held massive unauthorised trading positions, placed by Star Trader Nick Leeson, which would be exposed as the Nikkei 225 began to fall. Leeson had been placing unauthorised bets on the Nikkei 225 index in both Japanese and Singapore markets for 3 years without detection.

Leeson reported fictitious profits of £9mio for 1993, £25.5mio for 1994 and £18.5mio in 1995. These "profits" amounted to half of Barings Singapore's 1993 profits and half of the entire firm's 1994 profits.

The real financial picture was one of increasing losses, amounting to £21mio in 1993, £185mio in 1994 and £619mio for the first 2 months of 1995, before the Bank was forced into Liquidation on 26 February, 1995, hundreds of years after it was first founded (1762) by and continuously controlled by members of the Barings family.

Leeson engaged in unauthorised activities almost as soon as he started trading in Singapore, moving from Barings London in 1992, making a £2mio loss in his first year and hiding this loss in a trading error suspense account. The loss was incurred by conducting proprietary trades for Barings which he was not authorized to undertake. He was supposed to be trading low risk proprietary arbitrage trades as well as executing client orders on both Japanese and Singapore exchanges. This arbitrage strategy, which Barings called 'switching', was intended to take advantage of a market anomaly where temporarily the prices for certain contracts (specifically Nikkei 225 contracts traded on SIMEX and on the Osaka Stock Exchange (OSE) were different. When these price differences emerged, Leeson

would be authorised to quickly buy on one exchange at the cheaper price and sell simultaneously the more expensive one before the prices came back to parity. This kind of arbitrage strategy should have little risk because positions are matched. In order to make money large purchasers and sales would however be required. As far as client transactions were concerned Leeson would execute these on the exchange for clients and charge a fee or commission and the risk of price movements would remain at all times with the clients.

Unfortunately for Barings, Leeson was not only engaged in the "switching" and client execution business but additionally in highly risky proprietary position taking. For example most of the ultimate losses, which brought down the Bank came from Leeson selling put options and call options with the same strikes and maturities. This strategy is known in the market as a "straddle."

On the day prior to the Kobe earthquake, Leeson had large straddle positions that would make Barings money if the Nikkei 225 Index continued to trade in a range of 19,000 - 20,000. On the day of the quake, 17 January, the Nikkei 225 was at 19,350. The Markets reacted negatively and sent the Nikkei down, with Traders worried about the costs to Japan and to Japanese Companies from the effects of the quake. The Nikkei ended that week slightly lower at 18,950 so Leeson's straddle positions were starting to look problematic. The call options Leeson had sold, which would benefit the buyer in case the Nikkei rose above 20,000 were beginning to look worthless and so the premium received on these calls sold could likely be banked as profits. However, the put options sold, would become very valuable to their buyers if the Nikkei continued to decline. Barings losses on these puts were unlimited and totally dependent on how far the Nikkei would fall. The premium earned on the sale of these puts would be easily eaten away by the compensation Barings would have to pay.

Rather than accept the distinct likelihood of taking major losses with a Nikkei 225 falling further and fast, and instead of minimizing his losses (for example by covering his long position with sales of the Index) Leeson decided on 20 January to make major purchases of the Index, either because he thought the market had over-reacted to the Kobe shock and would bounce back or because he wanted to try to move the market back up and by acting in this way so reducing his likely losses.

The manoeuvre failed. Leeson was swimming against a tide of negative Japanese market sentiment and there was nothing he could do could stop it. The Nikkei dropped another 1000 points to 17,950 on Monday

January 23 and Leeson found himself showing losses on his two-day old long futures position and facing now even bigger losses on the put options he had sold. Over the next three weeks, Leeson doubled this long position to reach a high on 22nd February. The large falls in Japanese equities, post-earthquake, increased so called volatility in the market. For options, increases in volatility are beneficial to buyers. This is because the likelihood of the Nikkei being outside the range of 19,000 - 20,000 say in 3 months time had significantly increased due to the changes already seen in the market reacting to the effects of the earthquake. This would lead to increased losses for Barings as a seller of options (the calls and the puts) as a seller wants volatility to decline so that the value of the options decrease and of course the buyer is predicting the reverse.

Barings eventually could not meet the enormous trading obligations, which Leeson established in the name of the bank. The size of the positions built up by Leeson required massive funding from the Bank and the scale is underlined by the fact that in January and February 1995, as the positions grew and the losses mounted Barings transferred US\$835mio to its Singapore office to enable Leeson to continue to trade (Leeson was obliged to post collateral on Simex for the growing losses.) With reported capital of about US\$615mio for Barings as a whole the scale of the funding was astonishing.

Realising the game was up Leeson fled both Barings and Singapore on 23 February. Losses eventually reached £827mio (US\$1.4bio), twice the bank's available capital. After a failed bailout attempt, Barings was declared insolvent on 26 February. Leeson travelled to Malaysia, Thailand, and finally Germany where he was arrested at Frankfurt Airport after a short international Manhunt. Leeson pleaded guilty to two counts of "deceiving the bank's auditors and of cheating the Singapore exchange", including forging documents. Sentenced to six and a half years in Changi Prison in Singapore, he was released from prison in 1999, having been diagnosed with colon cancer, which he survived despite poor forecasts at the time.

Whilst Leeson admitted his guilt and has been punished for his crimes, the Singapore authorities in their published report on the incident were scathingly critical of Barings management, claiming that senior officials knew or should have known much more than they did, blaming the bank's internal auditing and risk management practices.

At Barings risk management failed spectacularly. For example, the management of Barings failed to establish

and maintain an independent operations function. The need for separation between those making trading decisions and those settling trades is perhaps the most important risk management principle. This lack of segregation removes a critical independent and necessary check. An effective back office function will record, confirm and settle trades transacted by the traders, it will reconcile them with details sent by the bank's counterparties and will assess the accuracy of prices used for its internal valuations. It also accepts/releases securities and payments for trades. Some back offices also provide the regulatory reports and management accounting. As such the back office provides the necessary checks to prevent unauthorised trading and minimizes the potential for fraud. Since Leeson was in charge of the operations back office, as well as responsible for trading he had the final say on payments, incoming and outgoing confirmations and contracts, reconciliation statements, accounting entries and position reports.

Abusing his position as head of the back-office, Leeson used an internal suspense account in Singapore to cover his tracks. The account was set up in July 1992 and was used by Leeson claiming to the Singapore exchange that it was a London client behind the account and not Barings, and removing the account from reports to Barings Management so they couldn't see the mounting losses and so perpetuate the myth of continued profitability in Singapore. Suspense accounts are not uncommon within Operations departments and are used for a number of reasons including for example to house trades that cannot be reconciled immediately. These accounts should only be used on a temporary or ad hoc basis and all trades should be properly allocated and reconciled with legitimate accounts. These accounts should not be used by traders and reports of activity on these accounts should be reviewed by management. The particular account used by Leeson gained additional fame as it was named and numbered account '88888', so styled after the number 8 seen as a lucky number in Asia.

With a trader also responsible for the operations back office function, there is a significant danger of unauthorized and or fraudulent activity occurring. It is still possible to avoid problems nevertheless or at least to identify them at a relatively early stage if remaining controls are effective. For example, a bank is required to have an internal audit department that reviews in detail areas of the banks activity and operations, a banks management is meant to closely supervise the activities of subordinates, the treasury department of a bank must be prudent when it comes to financing the bank's activities, the credit and market risk department should

manage the bank's financial risk taking, the compliance department similarly when it comes to compliance with laws, regulations and internal policies and a bank should listen to concerns raised in the market or from exchanges about the sizes of positions. Last but not least a bank's regulators should effectively supervise the bank, its activities and be assured of its overall risk management and controls.

Not everything failed at Barings but even when things were identified, these red flags were ignored or not sufficiently acted upon. For example, an internal auditor's report in August 1994 concluded that Leeson's dual responsibility for both the front and back offices was "an excessive concentration of powers." The report warned that there was a significant general risk that Leeson could override the controls. The audit team recommended that Leeson be relieved of four duties: supervision of the back-office team, cheque-signing, signing-off SIMEX reconciliations and bank reconciliations. Leeson never gave up any of these duties.

Penalty: sentenced to 6.5 years in prison in Singapore

Actions: Barings went bust after losses of US\$1.4bio

Country: Singapore

Key date: 1995 (Kobe earthquake rocked markets and Leeson's positions)

Toshehide Iguchi

On 13 July 1995 Iguchi, then Executive Vice President of Daiwa's New York Branch and head of its Securities Custody Department, sent a personal letter to "Mr Fujita", the President of Daiwa, at Daiwa headquarters in Osaka, Japan. In the letter, Iguchi would confess that in trying to cover up a US\$70,000 loss made in 1983, he had caused a US\$1.1bio loss from unauthorised proprietary trading and unauthorised sales of clients' holdings in US Treasury Bonds. Iguchi further stated that he believed Daiwa should "keep the secret until the Bank and possibly the Japanese authorities could take appropriate measures." Born in 1951 in Kobe Japan, Iguchi moved to the US to complete his education. He studied at Southwest Missouri State College (now called Missouri State University) where he graduated after five years with a low scoring major in Psychology, and a minor in Art. Upon graduation some sources have his first employment as being a car salesman. Still in 1976, Iguchi was hired by Daiwa's New York Branch within its securities depository section, where his main duty was to process securities account payments. By 1980 he had been promoted to the position of portfolio manager and just four years later, in 1984, he was put in charge of a new section of the New York Branch, heading up the US Treasury bonds desk. Daiwa had been a traditional

financial institution in every sense of the word, and had steadily grown from its inception in 1918 to becoming a leading Japanese financial institution and then from the mid 1970s Daiwa increasingly turned to securities trading.

Whilst the losses were shocking what came next compounded the problems for Daiwa and would lead to the US authorities forcing Daiwa to close their business in the US. Daiwa management in Japan and in New York conspired to conceal the losses and instead of reporting the fraud to the authorities as they were legally compelled to do, the management went to incredible lengths, to cover up the losses. Daiwa, at Iguchi's suggestion, agreed to try to use its large capital reserves to replace the losses to clients by continuing to trade hoping to make profits and to replace the losses. Using fraudulent documentation, making false disclosures, pretending that Iguchi was on annual leave, so that an audit had to be postponed and even disguising the nature of his trading department, in order that it appeared as a back office function, Daiwa acted appallingly. It was only after it became apparent that the additional trading was producing continued losses and that this would be unsustainable that they instructed Iguchi to confess his crime to the US authorities. The US regulator barred Daiwa from operating in the US, whilst also fining it US\$340mio.¹⁹

By 1996 Daiwa had closed down its 15 US offices, selling US\$3.3bio of assets in the process. The effect on the bank was more lasting though with a revision to a deposit taking institution and a drastic reduction in their global presence. What was once a sizeable institution with a global presence had been reduced to a little more than a medium sized national bank. Iguchi was sentenced to four years in prison and after writing a number of best sellers for the Japanese market detailing how he undertook the fraud, is now commonly believed to be teaching English in a school in Kobe, Japan. A number of Daiwa senior executives were ordered to pay more than US\$750mio in compensation for losses incurred during fraudulent trading.²⁰

A court in Daiwa's home town of Osaka in Japan decided that 11 senior executives at Daiwa bore responsibility for their failure to supervise staff and detect the fraud, as well as their conspiracy to cover up the losses when they did come to light. "The risk management mechanism at the (New York) branch was effectively not functioning," presiding Judge Mitsuhiro Ikeda told the court. The case was brought by two Daiwa Bank shareholders. The executives have been ordered to repay a total of US\$775mio in damages to their own bank. The bulk of the award has been made

against the former president of Daiwa Bank's New York branch, Kenji Yasui, who has been told to pay more than US\$500mio. In 1984 Iguchi was put in charge of a new trading section of the New York Branch, heading up the US Treasury bonds desk. It was as a trader that Iguchi incurred a US\$70,000 trading loss which would set in motion a chain of events which ultimately led to his arrest, Daiwa's ban from operating in the US and a loss of US\$1.1bio. In order to make back the loss, Iguchi began to sell US Treasury bonds held by other clients, without their consent, hoping to use the proceeds of the sales to cover the original loss. Iguchi as both trader and a back office head was uniquely placed to carry out these illegal and unauthorised transactions, by booking the trades, processing and confirming them and then by altering the custody reports received from Custodian Bank, Bankers Trust he could sell the Bonds cover the loss and still show the custody positions as including the sold Bonds.

Unfortunately for Daiwa, Iguchi began losing money again and he quickly lost a few hundred thousand dollars, and again to cover these losses he sold off client Bonds from the Bankers Trust sub custodian account and forged documents to cover for the sales. During a period of eleven years, (1984-95) he is said to have forged some 30,000 documents. When customers sold off securities that Iguchi had, in fact, already sold off on his own behalf, or when customers needed to be paid interest on long-gone securities, Iguchi settled their accounts by selling off yet more securities and changing yet more records. The planning required for this deception also entailed creating false account statements for the defrauded clients in advance, in order that when Iguchi did go on holiday, which he rarely did, the client would only see their invented account history, and not the true condition of their account. In this manner Iguchi was able to quite literally retype both company's and clients' records to create a false reality.

By the end of 1984 Iguchi had lost US\$30mio, by 1988 US\$200mio and by 1993, US\$900mio. Eventually about US\$377mio of Daiwa's customers' securities and about US\$733mio of Daiwa's own investment securities had been sold off by Iguchi to cover his trading losses. Risk-taking functions must be segregated from record-keeping and risk assessment functions. This should have a very broad application. Firstly it should mean that no individual has the ability to perform both functions. Secondly, no individual should have access to systems which perform these functions simultaneously. Lastly it should be considered that those who have previously undertaken administrative functions may have sufficient understanding of how to circumvent controls which they themselves would have previously enforced.

Accordingly they present a higher risk to the firm when operating in a risk taking capacity. They should be monitored accordingly. Rules which enforce the risk management of the bank must be enforced without exception. This transcends preconceptions based on an individual's cultural background, their performance or standing in the bank. Inexperienced employees should not be providing oversight on desks where the bank itself has little experience. This risk is further exacerbated by the likelihood that the risk management controls may be theoretical in nature, and not robust enough to deal with a determined effort to circumvent them. Accordingly risk management controls must not just be based on theoretical models driven by regulatory requirements and expectations, but also by the inherent weaknesses in a bank's operations, as understood from the back, middle and front office, which deal at various levels with the same product. Both internal and external audits failed to identify the fraud. Given that this desk was involved in the growth area of finance in the 1980s, it might be considered that it warranted greater scrutiny, given the exposure it carried.

Accordingly it should be considered that the significant loss or profit making departments of an institution should warrant greater oversight from audit on an ongoing and continuous basis. Given that the events occurred over the course of eleven years, and that it appears that Iguchi at least originally acted out of fear of losing his job, rather than out of greed, it may be assumed that he would have displayed significant signs of stress.

Whilst this is to be expected in the occupation in which he worked, it may be considered that there was a failure in managerial oversight not just from the perspective of allowing Iguchi a range of responsibilities for both back and front office, but in not questioning why a seemingly successful trader (towards the end of his career at Daiwa Iguchi was reportedly producing half the profits of the entire branch) was becoming increasingly distressed. Finally, the role of management in concealing the fraud demonstrates the importance of senior management in dealing with misconduct both decisively and with full transparency.

Iguchi himself had a different take on the responsibility for this incident which he set out in his book published following his release from Prison. Iguchi wrote, "Although corporations are criticised for their failure to have proper internal controls, traders are prosecuted for causing the loss. In the eyes of the public, the rogue trader is the only culprit. When he's sent to prison, the case is closed. He is being punished so he won't do it again. The problem is that no rogue trader thinks he

is going to lose a billion dollars, because it begins with a small loss, usually less than a hundred thousand. In reality, most financial institutions have now installed check-and-balance systems to prevent anyone from losing millions without being detected. If a trader loses more than he is allowed, he may do things he shouldn't in order to dig himself out, especially if one of the consequences of admitting a loss is losing his job. But he wouldn't even consider it if proper control measures were in place. Institutions must take responsibility for deterrence if they engage in the trading business. The management must take any loss from unauthorised trading as its own loss and not be allowed to call itself a victim. Many people who read my book in Japan maintained that traders like Yamada, Mizuno, Takagy, and me were the victims of Daiwa's lack of effective controls. Trading is a tough business. To trade well, one must often go against human nature. In doing so, one must ignore inner warnings and take a course that seems self-destructive. It's much like turning the wheels of a car toward the direction of skidding. It takes enormous discipline to do this day-in and day-out. Traders are constantly tempted by inertia to stay on the safe side. In the course of business, all traders make erroneous judgments and lose money, especially the many junior traders who fall into traps that are set by those who are much bigger and wiser. If the institution has strict internal controls in place, they are likely to lose their job. It's a merciless world. There are no other jobs like trading. Because of its nature and the psychological pressures traders are under, the least an employer can do is to not give them the chance to consider unauthorised activities. Passing out severe sentences will not deter them from rolling the dice one more time if they can, when that's measured against the disgrace of losing their job. On the other hand, making management culpable will force it to implement effective controls, so we will not hear another case of a 'rogue trader'."

Country: US

Key date: 1995 (confessed to US\$1.1bio losses for Daiwa)

Kyriacos Papouis

In 1997, NatWest Markets (NWM), the corporate and investment banking arm of one of the UK's largest banks, National Westminster Bank now part of the Royal Bank of Scotland Group revealed that a £50mio loss had been discovered in its interest rate options and swaptions trading books. The loss figure escalated to £90.5mio after further investigations.

NWMs troubles started with a systematic mispricing of various options and swaptions by traders in its rate risk management group. As losses mounted, Kyriacos

Papouis, a 29 year old trader who traded Deutschemark (DEM) interest rate options and swaptions, began to mismark options positions in the banks books in a concerted attempt to cover up the losses. His supervisor, Neil Dodgson, who traded Sterling (GBP) interest rate options and swaptions, also mismarked positions and was later found to have lacked the due skill, care and diligence required of him by UK regulators. Investor and shareholder confidence in the management of NWM was severely shaken and, in June 1997, Martin Owen, the head of National Westminster's investment banking group, also resigned. Rightly or wrongly, confidence was shaken so badly that in July 1997, the Bank of England had to instruct NatWest to resist calls for the resignation of its most senior executives in an effort to draw a line under the affair. The banks internal controls and risk management were questioned and severely criticised in May 2000, after a lengthy investigation.

The regulator imposed a penalty of £420,000 on NWM, and fined and reprimanded Papouis and Dodgson for breaches of UK Regulator's principles. But the real damage was to the reputation of National Westminster Bank itself, and with confidence undermined, the Bank fell in a hostile takeover in February 2000 to the much smaller Royal Bank of Scotland. In addition, Papouis was found to have violated principles of integrity and fair dealing, while Dodgson was reprimanded for not acting with due skill, care and diligence, however the investigations did not suggest that there had been widespread collusion at the bank, or that the mismarking had been conducted in the pursuit of personal gain. Both Papouis and Dodgson were fined by the SFA, to the tune of £50,000 and £5,000 respectively, and Papouis was expelled from the industry in the UK. Its not entirely clear how Papouis made his initial mistakes in options pricing, but it is clear his losses mounted steadily as the markets moved away from his mispriced options portfolio.

The UK Regulator estimated that Papouis' losses escalated from £1.1mio in March 1995 to £7.96mio in late-June 1995, and to £22.4mio by late-December 1995. The relatively slow escalation of the losses shows that NWM had plenty of time in which to halt the traders' actions. Furthermore, at this point, most of the losses were related to exchange-traded DEM options. These losses should have been relatively easy for NWM's back office to spot, given the discrepancy between any values in the bank's systems and readily available market price data supplied by the exchange.

Country: UK

Key date: 1997

Peter Young

Peter Young was a fund manager for Morgan Grenfell Asset Management, trading for three large European funds seeking international exposure. Morgan Grenfell was owned by Deutsche Bank who bought the business in 1989 from Mercury Asset Management. Young had made good profits on speculative investments in unlisted stocks in previous years and he continued to ramp up risk in order to maintain his run. To get around fund regulations that stated a fund could own only 10% of any company, Young created a mirror holding company through which to buy a major stake in a company he wanted. He proceeded to hold 10% of both the mirror holding company and the stock he originally targeted. Further, Young went on to use similar methods to circumvent the 10% limit on the amount of the fund that could be put into unlisted stocks. On top of illegal speculation, Young also used a system of warrants and dummy companies to filter the fund's money into his own personal account. Morgan Grenfell became suspicious when one of Young's investments, Solv-Ex, came under SEC and FBI scrutiny for possible violations. Despite the news and the resulting massive sell-off of Solv-Ex, Young went through with plans to buy the company's shares at a premium.

Morgan Grenfell suspended the equity funds that Young was running and began an inquiry. It found that Young was holding over three times the legal limit in unlisted shares and the bank hurried to cover the losses by closing out positions. One of the companies in the fund, Russ Oil, turned out to be wholly owned by Peter Young. He used it as a way to steal money from the fund to pay for his lifestyle. Young was sacked and later charged for conspiracy to defraud investors. The trial became highly publicized when Young wore dresses to the hearings and asked to be called Elizabeth. In 2002, the former fund manager was found unfit to stand trial and was in the hands of professional carers. Deutsche Bank is said to have lost around £400mio as a result of Peter Youngster actions.

Country: UK

Key date: 1997: (Peter Young fired from MG and charged with conspiracy to defraud investors)

Yasuo Hamanaka

On his release from prison in 2005 Yasuo Hamanaka expressed surprise at how the price of copper had risen while he had been incarcerated. This is the man who, at the height of his powers, was known as "Mr Copper" or "Mr 5%" due to the amount of the global copper market that he was believed to control. This is the same man who lost his employer, Sumitomo

Corporation, US\$2.6bio nine years earlier following a decade of fraud and forgery. To this day, aside from admitting the forgery of trading documents, Hamanaka has not spoken a word to anyone about the trading practices that enabled him to artificially inflate the price of copper for 7 years. As head of Sumitomo's metal trading division, Hamanaka controlled approximately 5% of the world's copper supply. This may sound relatively insignificant given that 95% remained in the hands of others but copper is highly illiquid and it cannot easily be transferred around the world to meet shortages. For example, a rise in copper prices due to a physical shortage in one country will not immediately be replenished by shipments from other countries with an excess of copper due to the time it takes to ship the metal and the costs of doing so. These logistical challenges meant that even a 5% share of the world's supply is significant. In 1986 Hamanaka, previously a non-ferrous metals trader at Sumitomo, was appointed Head Metals Trader but the first three years of his tenure were disastrous. He bought and sold physical copper without success and attempted to cover his losses with parallel trades in copper futures. He opened a secret book, known only to him, where he booked his unauthorised trades and it is reported that throughout this period he forged signatures, falsified trading data and peddled lies to his superiors in order to maintain the veil of secrecy around his losses.

In 1989 Hamanaka met David Campbell, Head of Metals trading firm RST Resources, and devised a plan to recoup his losses and actually start generating profits by artificially inflating the price of copper. He would trade off the market; selling below the market, buying above it, and selling large quantities of over the counter options cheaply. This is known as "painting the tape". The prime reason for selling cheap options is to create current income to cover bad price trading. Over the next four years Sumitomo became RST's biggest client and then in 1993 David Campbell set up Global Minerals & Metals Corp. Soon after, Sumitomo ceased trading with RST and quickly became the biggest client of Campbell's new venture. The Fordham Law Review articulates the details of Hamanaka's scheme well: "Hamanaka and Campbell entered into a string of intricate agreements whereby Sumitomo agreed to make monthly purchases of copper from Global from 1994 to 1997. Ultimately the goal of these agreements was to establish the appearance of legitimate and genuine commercial need to obtain physical copper. Global would purchase copper warrants from a Zambian copper producer. Subsequently, Global would sell the copper to Sumitomo, and finally Sumitomo would complete the circle by selling the same amount of copper back to the Zambian firm. As a result of the

paper transactions, Hamanaka established a façade of legitimate business, thereby providing him with false commercial justification to establish a large futures position supposedly hedging the illusory delivery obligations.

The second step in Hamanaka's plan mandated the establishment of a massive futures position. In order to acquire the necessary futures contracts on the London Metal Exchange, Sumitomo opened an account with Merrill Lynch (the "B" account) under a power of attorney signed by Hamanaka, authorising Global to trade using Sumitomo's vast line of credit. This move provided Global, a thinly capitalised start-up company, with instant credibility and the necessary credit to purchase the large number of futures contracts needed to execute Hamanaka's planned course of action. Using the "B" account, Global began to establish a large long position in LME copper futures. By September 1995, Global acquired an open long futures position of 780,000 metric tons of copper. Through the use of other small brokers in combination with the "B" account, Sumitomo possessed two million metric tons of copper in the form of futures and owned nearly one half of LME copper warrants. At this point, Hamanaka began to unwind the futures positions by taking delivery on expiring futures contracts to further his plan to control the cash supply of copper and ultimately generate large profits. He masked this scheme under the guise of legitimate commercial need for physical copper. Merrill, through the "B" account, provided Global with the financing necessary to take delivery on the LME warrants. By November 1995, Sumitomo controlled virtually 100% of the LME warehouse receipts."

Hamanaka had not only obtained a dominant position in the cash market, but he also established a powerful long futures position. These positions would force traders who previously sold copper futures and who innocently waited until the end of the delivery period, to run to Hamanaka to offset their positions at prices that Hamanaka could virtually dictate.

According to various reports, Hamanaka's manipulation seemingly did not go unnoticed. Apparently many speculators and hedge funds knew that Hamanaka was long in both copper physical holdings and futures. Whenever anyone attempted to short Hamanaka, however, he would use the considerable resources of Sumitomo and inject more cash into his positions, thereby sustaining the price and outlasting the shorts. Hamanaka held long cash positions that forced anyone shorting copper to deliver the goods or close out their position at a premium.

Hamanaka was helped greatly by the fact that, unlike

the US, the LME had no mandatory position reporting and no statistics showing open interest. Basically, traders knew the price was too high, but they did not have exact figures on how much Hamanaka controlled and how much money he had in reserve. In the end, most gave up, cut their losses and let Hamanaka get his own way. Following the resurgence of mining in China in 1995, the market conditions changed. With the price already floating away from the fundamentals, the price of copper was significantly higher than 'real value'. Sumitomo had made significant profits on Hamanaka's price manipulation, but it was now left vulnerable because it was still long on copper at a time when the market was heading for a significant correction. To compound the matter, if Sumitomo shortened its position, i.e. by hedging it with shorts, its significant long positions would lose money faster because the company essentially had been playing against itself.

While Hamanaka and Sumitomo continued to wrestle with the dilemma of how to reduce their positions in an orderly manner, the LME and the Commodity Futures Trading Commission (CFTC) began investigating the manipulation of the copper market worldwide. At this point Sumitomo took the ill-conceived step of transferring Hamanaka away from his trading role. Given Hamanaka's reputation in the market, such a dramatic event was enough to send the price of copper through the floor. Sumitomo soon announced that it had lost over US\$1.8bio and that the losses could go as high as US\$5bio as the long positions were due to settle in such an unfavourable market. Sumitomo also claimed that Hamanaka was a rogue trader and that his actions were completely unknown to management. The common view seemed to be that Sumitomo must have been aware of Hamanaka's fraudulent activity because the company continued to supply money every time speculators tried to move his price. However, it could simply be that his matrix of trades was so complex that the firm, content with its resulting profits, were happy to continue to fund his positions.

Hamanaka was charged with forging one of his supervisor's signatures on a form and in 1998 he was convicted to 8 years in prison. He was released one year early in 2005. Sumitomo eventually disclosed a loss of US\$2.6bio and despite its protestations of ignorance, its reputation was significantly tarnished because it had profited for so long from the actions of one Yasuo Hamanaka. Hamanaka's pattern of trading became increasingly complex, increasingly large and more opaque. This process accelerated after 1993 though the use of various derivative contracts, i.e. futures, options and swaps. Given the leverage that these types of instruments can provide, Hamanaka's trading should

also have raised red flags both with his immediate supervisors and in the control functions such as Risk, Compliance and Finance. His volume of trading was primarily through small and newly formed brokerage firms with offshore locations. He represented a large portion of their business and the firms were extremely profitable. Again, from a credit risk perspective this fact should have alerted the firm to ask questions of his actions. Hamanaka granted powers of attorney over Sumitomo trading accounts to brokers and effectively lent Sumitomo's debt capacity to third parties. These actions are highly unusual and should have been an immediate red flag to senior management that questions needed to be asked.

Hamanaka is also reported to have had the authority to create brokerage accounts, bank accounts, execute loan documents, and authorize cash payments. In a robust control environment these actions would require multiple approvals from a number of different functions, such as Data Management, Settlements, Legal and Finance. Segregation of duties is one of the primary protections for any firm against fraud and clearly traders must never be permitted to authorise, let alone cash payments.

Unsurprisingly Hamanaka worked long hours, late into the night at Sumitomo, he turned down transfers, and he had a good reputation within the company. We can therefore assume that he was working late for some reason other than to gain promotion or a new role. Human nature is to focus on the poor performers and where money is not being made. This case, and others like it tell us that equal, if not greater scrutiny, should be given to top performers and those generating significant profits. HR policies must also be robust in order to detect this type of behaviour. Managers must be expected to notice if a member of staff regularly works long hours and takes almost no holiday. Sumitomo transferred Hamanaka away from trading to a new role on 17 May 1996 while it still had a large exposure to the price of copper. Prices fell 30% after the market became aware of the reassignment of "Mr Copper". Hamanaka confessed on 5 June and Sumitomo unwound some positions in the following days but ultimately incurred a loss to the tune of US\$2.6bio. This highlights how difficult it is for a firm to deal with the discovery of a rogue trader. Whilst being open and transparent with regulators and law enforcement authorities a firm must act very carefully in protecting its own interests and those of the market.²¹

Country: Japan
Key date: 1998 (conviction for 8 years in prison after losses of US\$2.6bio amassed by Sumitomo)

Joseph Jett

In July 1991 US based securities firm, Kidder, Peabody & Co, hired 33 year old bond trader, Joseph Jett, to work on their US Government Bond Trading Desk within the Fixed Income Division. With undergraduate and graduate degrees in chemical engineering from MIT and a 'Master in Business Administration' degree from Harvard, Jett's commendable academic background stood in stark contrast to his unimpressive employment history at that time, having been terminated from roles at both Morgan Stanley and First Boston in the prior three years due to poor performance in trading collateralised mortgage obligations. When first employed at Kidder in 1991, Jett's role was simple and his authority was limited, working to learn his trade working on the US government bond desk. This market involved the most liquid and actively traded market in the world, and as such provided limited profit opportunities. After several months of achieving insignificant profits, Jett identified a serious flaw in the KP computerised analytic trading system in which government securities transactions were entered. He realised that Kidder's trading and accounting system would allow unprofitable trades to appear profitable for a period of time. He would go on to devise "carefully planned trading strategy" to exploit this IT fault in order to generate millions in false profits, securing himself promotions and large bonuses.

However, this success was short lived. The "strategy" was ultimately unsustainable and would crumble to reveal more than US\$264mio illusory profits, and actual trading losses of US\$74.6mio and undeserved bonuses paid to Jett of US\$11.4mio. The regulators NYSE, SEC and NASD all took action against Jett, though no criminal charges were ever filed.

Jett was banned from the Industry but was initially only charged with a relatively minor record keeping violation, avoiding securities fraud charges in 1998 after a 4 year investigation. The SEC announced that "This Initial Decision finds that, for over two years, Mr Jett exploited an anomaly in Kidder's software, in the manner of a pyramid scheme, that credited him on Kidder's books with enormous, but illusory, profits. He did this with intent to defraud". The SEC ordered Jett to forfeit his US\$8.2mio in bonuses associated with the false profits, fined him US\$200,000, and barred him from any future association with a securities broker or dealer. Both Jett and the SEC's Enforcement Division appealed the decision. In March 2004 the Securities and Exchange Commission finally ruled on the appeal, and concluded that, in addition to upholding the record-keeping violation, Jett had also committed securities fraud.²² Specifically, they found that Jett committed

fraud by deliberately exploiting weaknesses in Kidder Peabody's automated trading records system in order to book fake profits of about US\$264mio (when he had actually lost the firm about US\$75mio). The Commission re-affirmed the penalty that Jett forfeit US\$8.2mio in fraudulently-obtained bonuses, plus the fine of US\$200,000 and a lifetime bar from the industry. The SEC started an enforcement action against Jett in 2007, ordering him to pay the fines due, though it is not known how successful they were.

Jett denied concealing the trades and put the blame on KP management, stating that the company knowingly engaged in fraud in an attempt to wrest control of KP back from GE. As a result of Jett's actions GE would ironically disengage from KP, when GE decided to exit this business following this and an earlier insider dealing scandal at KP (see the insider dealing case of Ivan Boesky below for details) selling KP to Paine Webber, since acquired by UBS.

Jett's primary strategy was to exploit a flaw in Kidder's computer systems that made unprofitable trades appear profitable. The few real trades he executed consistently lost money. The problematic trades involved US Treasury Bonds and the coupon or interest attached to them. Jett bought the coupons which had already been stripped from the Treasury Bond and reconstituted them back to the T Bond so that it returns to its original form. Kidder's system incorrectly valued forward-dated transactions as if they were immediately settled, rather than taking into account the time value of money for the period before settlement of the trade.

The method Jett followed was facilitated by this error. By buying US Treasury bond strips (whose price increases each day due to accretion), hedged by a short treasury bond position (whose price remains relatively stable over the settlement period), Jett was able to book immediate, illusory profits. The problem was that at the date of settlement in the future these profits were reversed and would instead then record a loss. Therefore, in order to continue to appear profitable, Jett had to engage in more and more trades, enough to both offset the losses on the settling trades plus additional trades to keep delivering profits. For the scheme to persist, the size had to continually grow, and in essence it became a pyramid scheme. It was the size of the trading that eventually brought it to an end. General Electric, the owner of Kidder Peabody at the time, had become concerned with the expansion of the KP balance Sheet and in September 1993 instructed KP to reduce the size. KP committed to reduce the Fixed Income Division's balance sheet inventory by US\$26.2bio which included reducing strips inventory by approximately US\$5bio

over the next year. This meant over time moving to close out some of Jett's existing transactions early which would then realize losses. Jett stepped up his trading activity significantly in January and February 1994, to counteract the closing out of existing positions in order to counteract the losses and still generate profits. By early March 1994, KP management became concerned about Jett's trading increases when the strategy was to reduce overall positions. The concern led to closer scrutiny which led management to realise that in closing out profitable trades early realized losses and the illusion was gone. Jett, who was previously a marginally profitable trader, started earning large bonuses once he began executing the trades that exploited the system flaw.

Jett was paid a bonus of US\$2.1mio in 1992 and US\$9.3mio in 1993. The board of General Electric, who had owned Kidder Peabody since 1986, had to approve the US\$9.3mio outsized bonus in 1993. Later, in his autobiography *Straight from the Gut*, Jack Welch would admit and lament not personally looking into how one of his employees could become so successful so quickly. As the scandal first came to light, Kidder Peabody hired lawyer Gary G. Lynch from the law firm of Davis, Polk & Wardwell, the former enforcement chief of the Securities and Exchange Commission, to conduct an internal investigation. The result was an 86-page document that became known as the Lynch Report.

The report was released in August 1994 and concluded that Jett acted alone, but also blamed the losses on a complete breakdown of the system of supervision at KP. "Jett was provided the opportunity to generate false profits by trading and accounting systems" Mr Lynch wrote, "It was his supervisors, however, who allowed Jett that opportunity for over two years because they never understood Jett's daily trading activity or the source of his apparent profitability. Instead, their focus was on profit and loss and risk-management data that provided no insight into the mechanics of Jett's trading."²³

Country: US
Key date: 1998 (SEC action against Jett for losses of US\$75mio at Kidder Peabody)

John Rusnak

From the mid-1990s Asian currencies, the yen in particular, did not fare so well over the dollar. In 1995, before the markets began to turn, Allfirst Bank in Baltimore hired John Rusnak as a foreign exchange trader. Rusnak began accumulating losses: US\$29.1mio by 1997, US\$300mio by 2001, leading to a total loss of US\$691mio in 2002. Rusnak traded, manipulated and

deceived between 1995 and 2002 before not showing up for work on Monday, 4 February 2002. It was the next day that the FBI were called in to investigate the activities of this rogue trader.

Allfirst Bank's Baltimore office was a small outfit. A subsidiary of Allied Irish Bank at the time, Allfirst hired Rusnak to grow the bank's foreign exchange operations, hoping for a considerable profit. They got what they hoped for on paper at least, as Rusnak worked hard to hide his spiralling losses using his knowledge of the weaknesses in the bank's systems, controls and supervision, creating the illusion of profitability. In fact, he left Allfirst open to significant liabilities. As the senior trader of only two foreign exchange traders at Allfirst, he enjoyed the kind of autonomy and control that would allow him to mount losses and cover them up continuously. Whilst he received bonuses calculated at 30% of his trading profits, he did not appear to have benefited financially in any other way from his activities.

Most of Rusnak's losses were accumulating whilst betting that the yen would appreciate against the dollar. In order to obtain a level of protection in these circumstances, a trader would normally buy forward contracts to secure yen for cheaper than the expected market value, whilst hedging the position with a combination of put and call options. An option is a contract that gives you the right, but not the obligation, to buy or sell something on or before a specified date at a specified price. Rusnak, full of arrogance and wishful thinking, did not hedge his forward contracts. He went about creating fictitious trades to make it appear he had hedged his position but in fact he had created huge liabilities for Allfirst that were not reflected on their balance sheets. Allied Irish Bank's profits for 2001 were cut in half as it covered the losses that Rusnak had made. Keen to continue his actual profitable trading when he started at Allfirst, Rusnak had purchased forward contracts believing that the yen would appreciate consistently against the dollar. When the opposite happened, instead of re-evaluating his trading strategy, he ploughed more of Allfirst's money, into yen's recovery. He believed it would happen, so he had to find a way of buying time, of covering his losses and avoid getting caught. To keep the bank from discovering his losses, Rusnak entered false options into the bank's systems to make it look as though his positions were hedged. When options are bought or sold, they are usually confirmed by the buyer or seller. The back office function would usually seek to obtain this confirmation. For the bogus options Rusnak had created, he convinced the back office that no confirmation was required. He

bullied the back office into accepting that as the deals offset each other, there was no net cash position: the first option would involve a receipt of a large premium and the second would involve paying out an identical premium. These options would normally expire on the same day, but that would not have helped Rusnak hide his mounting losses. The first option expired on the same day it was written, while the other option would not expire for several weeks, buying him time. He also stated that it was common practice not to confirm Asia trades as it would have meant getting up in the middle of the night to do so. An independent check on either of these issues would have shown a red flag and could have helped limit the loss.

The fictitious trades grossly misrepresented the value of Rusnak's trading and the risks and potential liabilities that would eventually manifest. When it was clear that this alone would not help his situation improve, he requested permission for a prime brokerage account from his superiors. On paper, he was making a profit and at the prospect of even greater profits, he was granted his wish, notwithstanding it was a highly unusual course of activity for any firms except the largest ones. Such an account allowed him much more capital to gamble with and would restrict the ability of the back office to interfere with his activities, with the prime broker in effect acting as the back office.

To further conceal his losses and try to buy more time, he used historical rate rollover contracts, which would allow him to hold off realizing his losses by extending the rate of the original contract to later date. Rusnak created the illusion that there were no losses. The balance sheet showed increasing amounts of capital being used for foreign exchange trading and it was when he was told by Allfirst's Head of Treasury in 2000 that he needed to reduce the amount being used that his deception began to unravel. At this time, foreign exchange trading revenue at Allfirst was US\$13.6mio, whilst net trading income was only US\$1.1mio. In order to continue in his attempt to recover his losses, he sold deep-in-the-money options with high premiums. These options acted as loans which he would have to repay after a year, when the options were due to be exercised, in order for Rusnak to buy back yen at a cheaper rate. He needed the yen to rise so he could buy at a lower rate. If it did, he would be able to generate real profits. Instead, the yen continued to fall. To hedge against this liability, he began to enter bogus options giving the appearance that Allfirst had repurchased the options. As the yen continued to fall, his losses continued to increase. As the strike prices for these options were so deep, it was extremely likely that they would be exercised, creating huge potential

and eventually actual liabilities for Allfirst. Yet neither anyone at Allfirst nor any of the counterparties involved raised any concerns. When he was pushed for a confirmation of his trades by the back office, he bullied and intimidated them into accepting his approach.

A lack of appropriate supervision of his activity and support for the back office meant that he went unchallenged for a long period. At the start of 2002, following a review by the Allfirst Treasurer, Rusnak's positions were closed down for a period; action which the Treasurer believed would identify any problems with Rusnak's trading. By this point, he had been trading for nearly seven years with almost complete autonomy. Rusnak was then challenged on trades that did not have the required confirmations. As he could not produce them, he took to forging confirmations purporting to be from Asian brokers, using a file on his personal computer called 'fake docs', where he kept names and company logos. The company Treasurer was not satisfied with the confirmations Rusnak produced. At the end of a week where Rusnak came closest to being found out, he promised to provide the name of a broker who could confirm 12 particular trades that had been challenged by the night of Sunday, 3 February 2002 when the Asian markets opened. He never did. He never returned to work at Allfirst.

For his endeavours, in January 2003 Rusnak received a seven-and-a-half year prison sentence, as part of a plea bargain with US prosecutors, serving just under 6 years and ordered to undergo drug rehabilitation and repay the US\$691mio he lost. The actual amount he repaid would be dependent on the amount of money he would make once he left prison, but including at least US\$1,000 a month for the five years of his probation. Six executives responsible for the oversight of Rusnak's activities were also dismissed, whilst Allfirst's Chairman and AIB's Group Treasurer resigned. There were many reasons that led to Rusnak accumulating such large losses. Following identification of his activity, Allfirst commissioned an independent report which was provided in March 2002. Whilst not having the full facts (the court case against Rusnak did not take place until 2003) the report highlighted significant concerns relating to Allfirst and AIB's ability to identify and manage the risks in its foreign exchange trading operations. They were found to have inadequately supervised Rusnak. Together with a lack of independent challenge and weak controls, Rusnak was able to exploit a number of loopholes.

There was no segregation of duties between front and back office as Rusnak was effectively able to control both. Back office staff and risk managers should

have been undertaking robust supervision and AIB should have had greater involvement in the foreign exchange business at Allfirst. In particular, Rusnak was able to take advantage of the lack of experience and authority of back office staff, who should have obtained confirmation of trades with Asian counterparties independently, rather than relying on Rusnak.

Policies and procedures were not reviewed regularly and Rusnak's working practices were largely outside of existing policies and procedures without suitable reprimand or remediation action. The arguments used by Rusnak, for example, when convincing the back office not to require confirmation of his trades, should have given rise to discussion as to whether policies and procedures were appropriate and whether management had enough knowledge of what Rusnak was doing. This apparent culture of non-compliance permeated Allfirst's treasury operations, where either controls were in place and not adhered to or they were missing altogether. On one occasion, Rusnak e-mailed a trader at another bank stating "I have come to you with a problem, we need to outsource our balance sheet funding". This admission to another bank that he needed more funds to finance the firm's trading activity should have at least caused that other bank to raise concerns. Presumably the opportunity to do business with Rusnak and the expectant profits stopped the trader at that bank from taking the issue any further. Rusnak was dealing with Allfirst's funds, trading on their behalf, rather than using client money. Known as proprietary trading, this is a high-risk activity. Financial institutions need strong controls in this area to prevent the kinds of activity undertaken by Rusnak. A small office such as Allfirst's Baltimore office would struggle to manage this in a way that would make the risk-reward calculation favourable without access to the breadth and depth of information, expertise and economies of scale of larger financial institutions.

Rusnak used his knowledge of banking systems and weaknesses in controls to perpetuate his rogue trading, with little challenge from any internal risk control or audit function. For example, he manipulated the Value-at-Risk (VaR) figures used to monitor his trading activities. VaR is the most amount of capital a bank can afford to lose in adverse trading conditions. Rusnak would manipulate the figures prior to them being distributed to the rest of the bank, to mask the fact that his allocated risk limit far exceeded the bank's limit. He also manipulated currency exchange rates that the rest of the bank believed came from the market.

Even when loopholes were identified, Allfirst did not take remediating action for over a year, in one instance refusing to pay US\$10,000 for a Reuters feed that

would have circumvented Rusnak's personal computer and meant he would not have been able to manipulate the figures prior to the rest of the bank seeing them. The internal audit function itself was ineffective.

In 1999, during an audit of the treasury operation, none of Rusnak's transactions were checked to see if they had the appropriate confirmations. A year later, only one of his trades was checked. Rusnak's supervision by management was inadequate. His management did not understand what he did or market practices in foreign exchange trading. They placed a huge amount of trust in his integrity and ability without undertaking sufficient independent checks or taking seriously claims by the back office. So much did they believe in him, that the bank allowed Rusnak to trade during his vacations and did not monitor his out of hours activities, where he spent considerable time trying to trade his way out of trouble. Whilst his losses were mounting, he never actually took the ten consecutive days off required.

Given Allfirst's weak control culture it is not surprising that a trader who showed five years of profitability was not scrutinised more closely. The AIB Group did not have sufficient oversight of its subsidiary's activities. They took a very "hands off" approach and it seems that as profit continued to rise, albeit losses were being hidden, they were happy with the Baltimore office. Nor did Allfirst take directions from regulators seriously.

In September 2001 the US Securities and Exchange Commission sent a comment letter on Allfirst's financial statement, inquiring into the cash flow related to foreign exchange activity. Rather than undertake an in-depth review, Allfirst merely directed internal audit to pay it increased attention on their next audit. Such a comment from a regulator should have led to escalation to the AIB Group and immediate action.

The chronology of Rusnak's fraudulent activity was littered with many opportunities for someone to raise concerns and action to be taken. Rusnak was able to exploit weaknesses in controls, get away with bullying and intimidating staff and was not reprimanded sufficiently for activity that his superiors knew was against internal policies and procedures. This case highlights the importance of the need to go further than paying lip service to internal control policies, to have independent controls and checks, for senior management to drive a culture of compliance across its organisations and for firms to ensure that they grow their businesses in accordance with law, regulation and market practice

Country: US

Key date: 2003 (Rusnak gets 7.5 years prison for losses of US\$691mio for Allfirst Bank in Baltimore) Liu Qibing

Chinese copper trader Liu Qibing was a trader for China's State Reserve Bureau, which accumulates stockpiles of commodities for the nation's needs. Expecting prices of copper to fall, Lui Qibing took massive short positions in copper on the London Metal Exchange. Unfortunately the reverse happened and prices rose dramatically when China's central bank began lending increased sums to real estate developers, many of whom needed the metal for wiring. Liu suddenly disappeared but it was reported that the Chinese government, who initially denied Liu's existence, eventually detained him and sentenced him to seven years in prison. His actions led to losses estimated between US\$200 - US\$1bio as the Chinese government had to close out the short positions, by buying copper for delivery at higher prices or using copper from its own stockpiles.

Country: China

Key date: 2005 (Chinese trader goes missing leaving significant copper losses for Chinese State Reserve Bureau)

David Lee

David Lee was a New York based trader, that by 2007 aged only 36 had risen through the ranks at Canada's fourth largest Lender, through Bank of Montreal's (BMO) US broker dealer subsidiary to become a Managing Director, responsible for the firm's commodity derivatives trading business. He had been employed at the firm since 1997, originally as an analyst and then in 2000 climbed up the ranks into trading, where he bought and sold natural gas contracts, futures, options, swaps and swaptions. At first Lee started trading on behalf of client accounts but he steadily moved to grow the firm's proprietary trading activity into what was to be the tenth largest trading book at BMO. By May 2003, Lee began overvaluing, or "mismarking", his legitimate trading positions by overstating their fair market value, which made his book look more profitable to BMO than it was. This would enhance Lee's position in the firm and entitle him to receive additional compensation, but would lead to losses of US\$650mio by 2007. To successfully mark his positions in his favour, Lee would need to find a mechanism to circumvent BMO's controls which were meant to ensure trading books were valued at a fair price.

BMO, in accordance with best market practice, required traders to mark their positions to market daily themselves but would also control these marks by comparing these to price quotes for similar positions

obtained from independent third-parties, thereby observing real prices in the market and verifying the traders marks, and thus therefore reflecting accurately market prices. Whether Lee found the solution entirely himself or it was part of an arrangement or whether he was induced is unclear. What is clear is that Lee couldn't have carried off the illusion of profitable trading at BMO without the support of Kevin Cassidy.

Kevin Cassidy was a convicted felon, convicted for wire fraud in 1987 for which he received one-year probation and the payment of restitution, for tax evasion in 1993 for which he received six months in prison, and credit card and money laundering crimes in 1993 for which he served 30 months in prison. Astonishingly he was still able to establish a Brokerage business in New York State, called Optionable Inc, of which he became CEO, fooling the authorities and hiding his past. Cassidy helped Lee circumvent BMO's independent price verification process. Under an agreement with Cassidy, Lee sent to Optionable price quotes for his positions that matched the self-serving, inflated marks that Lee used at BMO. At Cassidy's direction, Optionable brokers later reiterated Lee's price quotes, virtually unchanged, to BMO's price verification personnel in "round trip" or "u-turn" e-mails. The back office at BMO unsuspectingly took these quotes as fair independent prices to verify Lee's trading book.

The deception was finally uncovered in 2007 when BMO decided, following advice received from a review of their risk management practices, that they ought to rely on numerous brokers to value trades and mark positions and to move away from one market counterparty. When they did this they quickly identified that there were significant discrepancies between valuing Lee's options using Optionable's data and data from other brokers. When BMO's management became certain of Lee's activities it announced losses of approximately US\$650mio. In the four years from May 2003 to May 2007, BMO paid Lee compensation totalling US\$10mio while his supervisor Robert Moore received US\$13mio. BMO also paid Optionable "millions of dollars" in fees and commissions, with BMO becoming the largest revenue generator for Optionable, with estimates that it received more than 40% of BMO's brokerage business.

David Lee pleaded guilty in a New York court to inflating the value of his portfolio and conspiring with Optionable to hide trading losses from the bank. He was ordered to pay a US\$500,000 fine and was barred from the industry. Robert Moore was dismissed by BMO and banned from the industry by the Commodity Futures Trading Commission and fined US\$150,000. Kevin

Cassidy, was charged with numerous criminal offences and after initially contesting the charges he eventually changed his plea to guilty to a count of conspiracy to commit wire fraud.

Lee's improper trading activity meant deliberately inflating the value of his portfolio of derivative positions in OTC natural gas options to overstate the value. Like all derivatives, the trade in options does not directly result in the transfer of a physical commodity's ownership. The product itself is derived from the underlying value of the commodity; the actual trading activity is therefore around obligations over the underlying product; in this case natural gas options which are contracts that give the owner the right, but not the obligation, to buy or sell (depending on the type of contract) natural gas. The contract will be bought at a particular price and a predetermined maturity date. Derivatives may be traded over the counter (OTC) or through an exchange. OTC trades are transactions that are privately negotiated between a buyer and a seller of the derivative; it does not require an exchange or other central counterparty to clear the trade. It is often considered to be an unregulated market since the disclosure requirements are not at the same level as trades on an exchange, this is because the OTC market is comprised of other banks and hedge funds that are commonly considered sophisticated market participants. Since the trading and pricing of OTC trades occurs privately the reporting and visibility of each trade and the price is not fully transparent. All of Lee's trades, as with his fellow colleagues, were subject to individual limits imposed by BMO, in addition to limits placed around the counterparty to the trades based on its credit worthiness. The risk department at BMO then routinely monitored compliance with those limits.

Robert Moore, Lee's supervisor, was responsible for setting and ensuring that Lee remained within his trading limits. Part of his role also required him to ensure that all traders complied with BMO's internal policies and procedures. In order to monitor the value of all open positions, Lee was responsible for assigning values (marking) to each of his open position. The method employed by the desk was based on "mark-to-model" i.e. a mathematical formula/model was used to simulate the price of the open options. The model would be periodically calibrated to ensure its effectiveness. The calibration required by the bank's risk department necessitated its traders to collect broker price quotes from other market participants – such quotes would be obtained and retained in electronic form to be used in the model. The process was seemingly a means to independently value each trader's positions – a process that the bank followed on a bi-

monthly basis. If independence was fully achieved the process should have provided a reasonable comfort level that the trading book was valued in line with market prices and prices quoted independently by external sources (brokers).

All traders at BMO were required to obtain quotes from external brokers. The firm maintained a list of preferred brokers that it would utilise for the purpose of ensuring that its book were fairly valued for NYMEX listed natural gas options. Dedicated personnel in the BMO's back office function completed verification of the process by receiving quotes from brokers. Where differences existed between the trader's valuations and that of independent brokers the firm took steps to ensure prices were adjusted inline with its internal accounting practices. Thus, using this process the valuation of the trader's books could be adjusted up or down. Of course, if the value were adjusted downwards resulting in the estimated profits being lower than the trader's own marking would suggest, this would reduce the trader's bonus and salary expectations. Optionable Inc, was a preferred provider for the independent verification process and Lee used Optionable since 2003 knowing they would take and transmit to BMO's back office the misknowned prices. The back office department unsuspecting took these quotes as fair independent prices to verify Lee's trading book. As mentioned above it isn't clear who initiated the misknowning idea.

BMO in a civil suit issued later against Optionable indicates that the idea and inducement came from Cassidy in exchange for BMO increasing trading with Optionable. The extensive use and provision of gifts and entertainment also played its part, particularly in compromising Lee's supervisor Robert Moore. BMO claimed, "In order to encourage Lee to continue to participate in his fraudulent scheme with Optionable, and to encourage Moore to look the other way, Optionable and Cassidy plied Lee and Moore with gifts and inducements, including gambling vacations." Lee and Moore allegedly accepted an assortment of lucrative gifts, including: US\$650 in tickets purchased by Cassidy for Moore on 16 March 2004; A string of "expensive dinners" for Moore at the Foxwoods Resort Casino, a Manhattan restaurant and at the Mohegan Sun Resort and Casino on six occasions from 2004 to 2007; "Hundreds of dollars" at a men's grooming club in Manhattan for Moore and Lee on two occasions in 2005; Expenses topping US\$1,000 for Lee and Moore at the Borgata Hotel Casino & Spa in Atlantic City, NJ in November 2005; Pricey car and limo services for Moore on 7 March 2005, 1 June 2006 and 17 August 2006.²⁴

As with many cases of unauthorized trading or fraudulent activity, a major weakness is usually found in a lack of management supervision. Of course the corrupting nature of the relationship that existed between Lee's supervisor Robert Moore and Optionable's Kevin Cassidy, made it extremely difficult for Moore to view Optionable and Lee objectively. Moore routinely enjoyed gifts, travel, meals and money from Cassidy. These expenses were not business related and were not pre disclosed to BMO. They may not have been lavish individually but in aggregate they most likely could be so described and the type of entertainment was often inappropriate, for example they even included gambling vacations and money to gamble with for both Moore and Lee. Moore also knew that Lee's relationship with Optionable, like his, violated BMO's gift and entertainment policies and put them at conflict between their personal interests and the interests of their employer. Moore also allowed Lee to trade while Lee was on vacation despite internal policy requirements that prohibited such practices. It is a well documented principle that block leave by staff helps to identify fraud. The rationale is simple; if the staff member is not in the office performing their routine activity then other staff members have to provide cover. This simple step significantly increases the likelihood of malpractice to be identified and reported by other members of staff. The other major weakness related to the reliance by BMO on Optionable as a single source price verifier for BMO marks. BMO was foolish to rely on only one such source for OTC prices and in particular should have realized that with increasing business flows Optionable was not an independent source. Finally BMO could have done a better job in conducting its initial due diligence over Optionable, prior to establishing trading lines, bearing in mind Cassidy's past criminal record, however it appears that Cassidy was able to fool the authorities in New York State as well as NYMEX who in April 2007 purchased a 19% ownership interest in Optionable, including US\$5.1mio of Optionable stock owned by CASSIDY.

Country: US

Key date: 2007 (Bank of Montreal made losses of US\$650mio)

Jerome Kerviel

On Monday, 21 January 2008 fears that the looming recession in the US would spread to every other continent triggered a global crash in share prices. Large overnight falls on Far Eastern stock markets prompted a ripple effect through Europe, a day of panic selling left the UK FTSE 100 index down 323.5 points at 5578. or 5.48% representing the biggest one-day points fall in London's history and the largest percentage fall since the

9/11 (2001) terrorist attacks. In other markets, Japan's Nikkei index was down almost 4%, while Germany's Dax and France's CAC index both fell by 7%. Since the start of the year share prices had dropped by an average of 14%, with the near 900-point fall in the UK FTSE 100 wiping out all the gains of the previous last 18 months. This sudden event provided the catalyst which triggered the announcement on the 24th January that the French bank Société Générale, one of the largest banks in Europe was to write down a US\$7bio loss (€4.9bio) as a result of a rogue trading incident within their Global Equity Derivative Solutions (GEDS) Department. This represented the largest single loss recorded in the financial industry by a single trader.

The rogue trader behind the fraud was named as Jerome Kerviel, a relatively junior trader, allegedly earning a comparatively modest €75,000-a-year. Initial reports indicated that Mr Kerviel's responsibilities were limited to arbitrage of equity derivatives; an activity that sought to manage two portfolios of comparable size and composition. The portfolios should offset each other and residual income is generated by exploiting the pricing differences between the underlying stocks and the futures contract prices for that exchange. Therefore if Société Générale's other traders had bought into the equity markets, expecting a rally, he was responsible to hedge some of this market risk through trading index futures. His remit was to neutralise such market risk. Kerviel did not have any approval to take directional risk, i.e. create open trading positions in the market.

Jerome Kerviel had joined Société Générale in 2000 having graduated from University Lumière Lyon with a Master of Finance degree specializing in organisation and control of financial markets. Kerviel joined the middle office of the bank Société Générale in the summer of 2000, with responsibility for trade monitoring. In 2005 he was promoted to the bank's "Delta One" products team in Paris where he was a junior trader. Société Générale's Delta One business included programme trading, exchange-traded funds, swaps, index futures and arbitrage trading. Kerviel earned a bonus of €60,000 on top of a €74,000 salary in 2006, considered modest in terms of the salaries paid to traders in the financial markets. He had hoped for a €600,000 bonus for 2007 and would have received at least half that amount. Investigations carried out by Société Générale concluded that during 2006 Kerviel began making fraudulent transactions that were considered to be precursors to the fraud. At the end of January 2007 Kerviel had built up a significant short position on DAX futures, estimated to be €850mio, this coincided with the departure of his former desk manager. By end-February 2007 this

had grown to €2.6bio and by end-March 2007 more than doubled to €5.6bio. By mid July a peak of €30bio was reached before the position was cut and rebuilt from September onwards. At the same time Kerviel continued his fraudulent activity by holding globally short positions on single shares. From mid-September to early-November the total size of his positions extended to over €100mio and finally reached a maximum of approximately €350mio. From November to December 2007 Kerviel began to unwind his positions on DAX and EUROSTOXX futures, such that by 31 December his fraudulent index positions were zero. Whilst some notable losses were recorded at the close of the year €1.5bio in profits were realised. January 2008 saw Kerviel build a €49bio long position of index futures, that was discovered on 20 January and unwound between 21-23 January leading to losses of €6.4bio, (€4.9bio after the €1.5bio profits are included). The EUREX exchange is suggested to have enquired as to why Société Générale had a significant Open Interest position (open interest being a relative percentage of the open contracts in futures on an exchange)

During early 2007 Kerviel began using various techniques to conceal fictitious directional risk taking trades including; cancelling positions and earnings generated by fraudulent positions, recording equal and opposite paired trades using off market prices but concealing losses generated. Entering false provisional cash flows to mask the fraudulent losses. This was an option that was supposed to be used by trading assistants to correct "modelling bias" by entering positive or negative provisions modifying the revaluation calculated by front office systems. It was concluded that Kerviel was well aware of the accounting practise that the use of provisional flows was only reviewed at month end, and thus cancelled any such flows prior to the control being completed. Kerviel regularly cancelled fictitious trades before they gave rise to any confirmation, settlement or control, with his previously gained in depth knowledge of the systems processes and controls gained whilst in the middle office he was able to use features that left him time to cancel such trades and replace them with new false trades. Such trading also included booking fraudulent transactions using "technical counterparties" typically used when a trader is waiting for the name of a counterparty from a broker or awaiting completion of a client set up in the front office system. Typically once questioned by either middle office or Operations Kerviel would cancel such trades, thus from an accounting and settlement perspective all appeared in order. Fraudulent trades were also created using a deferred start date (i.e. with a value date much in advance of the trade date) but which are confirmed only several days before value date, in accordance with

generally accepted market practice. Internal and external investigations reviewed the processes and controls around Kerviel's activities and his supervisions, and highlighted a number of significant failures. Throughout January to April 2007 Kerviel was not the subject of any specific desk supervision as the desk head had left and from April 2007 the new desk head did not complete any analysis of Kerviel's activities. Kerviel had also been reluctant to take any vacation, which whilst raised formally by the desk manager including during yearly appraisals nothing was ever done. Desk management had also failed to complete any in depth review of trading activities or analysis of earnings generated by trades or traders or their positions. Further to this when questioned by risk and operations for explanations around unusual trades, cancelled trades or unmatched trades against counterparties, Kerviel's explanations were taken at face value or such questions were disregarded and general excuses were made without any substance or follow up. Further to this, multiple persons were often involved with such concerns therefore no one person would be in full possession of the facts around a problem. This assisted Kerviel, allowing him to cancel or amend any suspicious activity.

Risk and Management also failed to exercise appropriate controls over the use of dummy counterparties and the use of cash flow adjustments. No review or analysis was undertaken of transactions cancelled, amended or suppressed from flowing from front office to risk and operations. Initial margin is payable on the difference between the market price and the strike price for futures contracts, such margin calls for the GEDS desk were abnormally high as were collateral costs, however neither the Delta One manager nor Kerviel's desk manager had visibility of such costs. Further, the middle office function responsible for margin, deposit or collateral requirements failed to identify Kerviel's sizeable positions as it did not complete any control over the aggregation of such positions to identify where such positions originated. As positions were aggregated only globally, the globalised treatment of such margin calls did not allow for the detection of the significant amounts paid and received related to Kerviel's activities.

The Société Générale loss redefined the potential impact of an operational risk loss event. As a result the key European Regulators (FSA, FINMA, BAFIN) reminded financial institutions of the key areas of focus particularly related to preventing rogue trading including; internal assurance control framework should be comprehensive and operate effectively; Basel II Advance Measurement Approach calculation to include a rogue trader stress scenario; appropriate segregation of duties, both systemically and physically

controlled, between risk taking, risk management and operations processing and settlement functions; excessive risk taking and non-adherence to risk (or other) limits to be identified, escalated and management action taken: Regulatory imposition of "Block Leave" requirements for persons deemed to occupy sensitive roles (e.g. traders); exchange limits are captured and monitoring, specifically around open interest limits; timely processing, settlement and confirmation of such financial instruments; effective management supervision controls over the use of "dummy counterparties and "Risk only" trading portfolios; effective risk and management review of transactions cancelled and amended; and unusual and excessive margin or collateral calls should be escalated to appropriate management.

Country: France

Key date: 2008 (losses announced of US\$7bio for Soc Gen)

Frances Yung

In 2008, the Chairman of Citic Pacific, (a Hong Kong diversified company, and a subsidiary of China's Citic Corp focussing on special steel manufacturing, property and iron ore mining, which supplies the raw material needed in the making of special steel and property development in mainland China), Larry Yung disclosed that the firm lost more than HK\$15bio (US\$2.3bio) due to "unauthorised currency trades". The board became aware of this on 7 September 2008, and disclosure was made to the financial markets after trading in its shares was suspended on 20 October. When the shares resumed trading, the share price had fallen by some 75% since the previous close, and would lead to the resignation of the Chairman and other senior managers. Citic Pacific said that the currency bets, made by the company's financial director and overseen by the financial controller, were unauthorised. Among those involved in the disastrous trades was Yung's 37-year-old daughter Frances, who, along with Yung's son, Carl, soon after left the company.

The events that led to Larry Yung's resignation was a remarkable downfall for the former richest man in mainland China (Forbes:2005). Larry Yung, was the son of Rong Yiren, a former vice president of China from 1993 to 1998 both members of a famous family, widely considered as China's first major entrepreneurs. The family's owned flour and cotton mills were nationalized by the communist government in the 1950s. Rong served as an economic adviser to the Communist Party under Deng Xiaoping and helped enact the pro-market reforms of the 1980s. Rong set up state-owned China International Trust and Investment Corporation, now known as CITIC Group, as a vehicle to co-ordinate the

massive foreign investment needed to jump start the economy. He was appointed to the largely ceremonial but prestigious position of Vice President in 1993. As his father prospered, Yung moved to Hong Kong in 1978 and started an electronics business, later joining CITIC in 1986 before leading the takeover of an existing listed company and renaming it CITIC Pacific. The deal created one of the first "red chips," mainland-controlled companies with shares traded in Hong Kong. CITIC Pacific made many acquisitions and grew aggressively and as the Company grew, the Yung family's links to CITIC deepened. Two of his children, son Carl Yung Ming-jie and daughter Frances Yung Ming-fong, joined the Company in senior positions.

Country: Hong Kong, China

Key date: 2008 (Citic Pacific announced losses of US\$2bio due to unauthorised currency hedges)

Kweku Adoboli

In September 2011, UBS announced that it had lost over US\$2bio, as a result of unauthorized trading performed by Kweku Adoboli, a director of the bank's Global Synthetic Equities Trading team in London. On 24 September 2011 Oswald Gruebel, the CEO of UBS resigned "to assume responsibility for the recent unauthorised trading incident". On 5 October Francois Gouws and Yassine Bouhara, the co-heads of Global Equities at UBS, also resigned. UBS stated that no clients funds were lost as a result of the scandal, but the amount lost was almost the same as the savings UBS had planned via the elimination of 3,500 jobs. Whilst the loss to UBS was described as "manageable" and indeed UBS were even able to record a profit for the quarter, on the day of Adoboli's arrest, the price of the stock of UBS closed down 10.8%, while the price of other European bank stocks rose between 3-6%. It has been reported that Adoboli informed UBS of his unauthorised trades, and then the bank informed the UK Regulator and the police. On 16 September, City of London Police charged Adoboli with fraud by abuse of position and false accounting. On 18 September 2011, UBS issued a statement which revealed the losses from the alleged unauthorised trading stood at US\$2.3bio. The rogue trader reportedly racked up the losses by speculating on EuroStoxx, DAX and S&P 500 indexes. Kweku Adoboli was born 21 May 1980. His family home was in Tema, Ghana, but he had lived in the UK since 1991 and been described as "British by culture, citizenry and fame." He graduated from the University of Nottingham, where he studied computer science and management, in 2003. Prior to this, he studied at Ackworth School (a Quaker-run private boarding school near Leeds), where he was Head Boy between 1997–1998, the year he graduated. According to the

Daily Telegraph, shortly before the news of the incident broke, Adoboli had posted on his Facebook account that "I need a miracle".²⁵ Kweku's father, John Adoboli, is a former Ghanaian official at the UN. On the day of his son's arrest, he expressed the family's shock and disbelief: "We are all here reading all the materials and all the things being said about him. The family is heartbroken because fraud is not our way of life."

As mentioned, Adoboli worked on the Exchange Traded Funds desk in the Global Synthetic Equities (GSE) department at UBS in London in the Investment Bank. Whilst joining as a graduate trainee, he worked in a number of positions including for a time in the middle office in operations before joining the front office as a junior trader working his way up to become a senior trader.

Between October 2008 and September 2011, he executed a series of unauthorised trades which, when discovered, resulted in a loss to the bank of over US\$2.3bio. Adoboli amassed unhedged positions which far exceeded his risk net delta limits. He concealed the exposure to the bank by using a number of different mechanisms, by booking fictitious, offsetting trades, extending settlement dates, and hiding the extremes of the profits and losses the trades produced in an off-book account ("the umbrella account") from which profits and losses were drip fed back into the desk's legitimate systems.

Following Adoboli's arrest, UBS instructed an external advisory body to prepare an independent report into risk controls at the bank. The report identified a number of deficiencies, in the front, middle and back offices which were also largely accepted and formed the basis for regulatory action against the Bank by the UK FSA and Switzerland's FINMA in November 2012.

These included: (i) IT systems designed to assist in identifying rogue trading were inadequate; (ii) significant deficiencies existed in the trade capture and processing system. The system allowed trades to be booked to an internal counterparty without sufficient details and there were no effective methods in place to detect trades at material off-market prices and there was a lack of integration between systems; (iii) the Operations unit did not properly perform their role, rather than challenging the traders where appropriate, they perceived their function as being to assist traders in reconciling trades, accepting their explanations for breaks (a trade which would not reconcile between one system and another, or between one counterparty and another); (iv) there was inadequate front office supervision, for example, following the transfer of the

ETF desk to the GSE division, oversight for the ETF desk was assigned to a senior trader in New York. When the Operations unit reported problems with reconciling external futures trades which had been late booked by Adoboli, the desk's supervisor accepted Adoboli's explanations without challenge; (v) traders on the desk (including Adoboli) regularly breached the risk limits set for their desk, though they were not routinely disciplined. On one occasion Adoboli was disciplined, but not before being congratulated for the profit he had made; (vi) between 2010 and the first and second quarters of 2011, the net revenue recorded by the ETF desk increased significantly, several times greater than the increase in the desk's risk limits and no explanation for this was sought; and (vii) profit and loss suspensions to the value of US\$1.6bio were requested by Adoboli during the course of August 2011 and were accepted without sufficient challenge or escalation. For more details see Part 2 Section 8.

This incident is all the more shocking as it followed the massive unauthorised trading event at Société Générale, where Jerome Kerviel lost the Bank €4.9bio in 2007. Following this incident the FSA published guidance in its issue of Market Watch in 2008 on measures to take to minimise the risk of unauthorised trading. These included: (i) monitoring whether a trader had a high number of cancelled or amended trades; (ii) considering whether those exercising control functions had sufficient understanding, skill and authority to challenge front office staff effectively when agreed parameters for activity are breached or when something else suspicious takes place; (iii) enforcing risk limits with disciplinary action where appropriate; (iv) understanding where the desk's profit and loss is coming from; and (v) having proper systems to reconcile trades, and to confirm internal trades.

In addition to this guidance the following additional guidance can be added. First, firms should invest in intelligent systems and review controls in order to ensure a proactive and proportionate response to risk across the business. The inherent risk is significant and the investment and resources applied to design and operational effectiveness of controls must be commensurate with this risk. This means, for example ensuring that the middle and back office functions are adequately resourced and sufficiently skilled and trained. Firms need to balance the generation of profit with not only adequate but strong risk management for significant risks.

Second, increasingly within financial institutions, the amount of information, that is produced, deafens those that are trying to listen for anomalies and red

flags. Large individual red flags are rarely identified, and individual smaller ones are rarely brought together to form a clear picture. This is exacerbated by the numerous actors involved in the control space, from supervision, to front office colleagues, to HR, finance, operations, risk control, IT, legal, compliance etc. Many of the warning signs or red flags such as the exceeding of risk limits or considerable increases in profit in a short space of time, or the failures to take action on so called misdemeanours, including personal account dealing breaches or failure to attend mandatory training sessions, or the failure to spot lying about his qualifications at the start of his employment, or the failure in an outsourced confirmation checking process, point to a broader issue, and one that is unlikely to be a challenge only at UBS. These individual infractions, breaches and/or violations and/or concerns were not investigated or considered alongside each other. A silo approach to risk management and control presented Adoboli with the opportunity to continue his unauthorised activity for far too long.

For example, during Adoboli's trial, the court heard that risk limits had been breached by Adoboli on various occasions. The court heard of an e-mail sent by Adoboli to John DiBacco, the manager of the exchange-traded fund (ETF) desk where Adoboli worked, in which he stated he had been "running around US\$200mio of deltas". This was double his risk limit, set at US\$100mio intraday. DiBacco's initial response was "well done", later replying "when over US\$100mio and certainly US\$200mio, I need to know before, not after". DiBacco, who was based in New York, was not aware however of most of the information concerning profit and loss, risk positions, or any cancelled, amended or late trades. This information was instead sent to the desk's former supervisor, Ron Greenidge, who was based in London and was European Head of Cash Equities at the time. Furthermore, information from the risk management sub-system "was not being fed to the supervisory portal through most of the relevant time when Adoboli was trading on his own authority. The court also heard that there had been a "substantial increase in profitability of the desk". In 2010, the ETF desk made a total profit of US\$11.5mio, the court heard - by the end of the first half of 2011, the desk had made over US\$60mio. Similarities can be found in the case of Jérôme Kerviel, the convicted rogue trader who caused a loss of €4.9bio to Société Générale in 2008. Managers were made aware he had generated €7mio in 2006 and €43mio in 2007, yet no alarm bells were rung. Adoboli had even requested profit and loss suspensions to the value of US\$1.6bio during the course of August 2011. A UBS Finance executive, who worked as a P&L controller for the ETF desk, acknowledged

in court that he had allowed such suspensions without further information or challenge. Signs of fraudulent activity can be as simple as a reluctance to take holiday, as was the case with Kerviel. In 2007 Adoboli took just four days' holiday, though later he did take his required holiday entitlement.

One of the major control failures to emerge from the trial, was the failure over long-dated settlement controls, which allowed Adoboli to enter into fictitious trades without being caught. The control was supposed to be triggered when a settlement date had been extended 14 days or more after the date on which a trade was confirmed. Whilst this control had been in place in 2008 and was one of the lessons learned from the Soc Gen, Jerome Kerviel case the control had been offshore and outsourced and in fact had not been functioning between November 2010 and September 2011. Moreover no-one had raised the alarm that the control was no longer in operation.

Thirdly and finally the most important guidance comes back to culture and the culture and effectiveness of supervision and the culture of challenge and professionalism within an organisation. No systems and controls are bullet proof, yet with an exceptional culture, high quality employee selection with integrity at the heart of the process and excellent supervision, the control framework need not be. In an era where the costs of compliance continue to rise and the need to build and invest in risk management and control systems, resources and programmes, in large part as a result of individual failures, are essential, the costs of non-compliance are much greater. Adoboli was eventually caught by a single relatively junior employee in the Finance department who refused to be ignored and asked the right questions and was not satisfied with the answers. Adoboli turned himself in, once he knew the game was up and that the firm was onto him. Many more had been close, knew a lot, or a little but chose to ignore the warnings, the behavior and the conduct. Another year without being caught and who knows how big the loss could have been.

Country: UK

Key date: 2011 (UBS announces losses of US\$2.3bio)

Private Banker Fraudsters

Hans Peter Walder

On the night of 24 September 2001, while celebrating his 30th wedding anniversary, Hans Peter Walder left the party handcuffed by 2 FBI agents and 2 Tarrytown, NY Police officers. The anticlimactic event took place

at The Castle which was owned by Walder, a veteran Swiss Private Banker employed at UBS New York, and his wife, Steffi. Guests were left stunned, shocked and in complete disbelief as to why someone like Walder would be escorted out by law enforcement agents. Unbeknownst to them, Walder had utilised his charm, knowledge of the banking system and influence among his colleagues to commit a major fraud in order to purchase the Castle and maintain a lavish lifestyle.

As a charismatic and trusted person, he was able to maneuver through existing controls, defrauding his clients and the bank of US\$73mio from 1992 to 2001. Hans Peter Walder was a seasoned veteran of the Private Bank. He had worked for UBS, in various international roles, for over 30 years and had developed close ties with his clients and senior management throughout the bank. The scheme required meticulous attention to detail and an understanding of operational controls and their limitations. Walder single-handedly committed the fraudulent transactions with no accomplice. The driving force behind the crime was the ownership of the Castle in Tarrytown, NY. He manipulated his colleagues, clients and family to feed his desire. The underlying theme with embezzlement is greed. It begins as a desperate measure with the intention to commit it as an isolated incident. The "thrill" of successfully executing the transaction without any repercussions or discovery, becomes the motivation behind subsequent and continued illicit efforts. The impulse spirals out of control the longer it is left undetected and allowed to continue.

The control environment during the time of his fraudulent activities allowed Walder to have total autonomy in various aspects of maintaining and establishing client relationships. Client Advisors were allowed to disburse client funds independently without additional supervisory approval; utilise existing documentation to open additional new accounts on behalf of their customers; and drawdown credit facilities without client or supervisory approval. In addition, the model at that time was such that there were no rigid controls over retained mail, verification of client disbursements or account openings etc., which led to Walder's abuse of the system.

A few years prior to buying the Castle, Hans Peter Walder was in a financial predicament and saw an opportunity to embezzle US\$700,000 from one of his client's effectively dormant accounts. However, the downside was when the client, eventually requested the transfer of the dormant funds to another account, this led Walder to steal yet from another client; which perpetuated into a domino effect of stealing from client accounts to cover up each prior abuse. Hans Peter Walder noted that he had become a prisoner of his own crime. His knowledge of the operational process enabled him to identify weakness in the system and exploit it to his advantage. It has been reported that for over eight years, Walder exploited his wealthy clients'

accounts, all for his own gains. From 1992 to 2001, a bulk of the proceeds of the fraud was for the purpose of refurbishing and operational expenses associated with the Castle in Tarrytown, NY. The obsession behind the ownership of the Castle and the status it provided him became the driving force behind the crime. Hans Peter Walder created a company named 400 Benedict Corporation which was the recipient of US\$69mio.

The discovery of the fraud occurred when Walder could no longer cover all his tracks, and the Bank identified a US\$15mio deficit. Upon discovering the fraudulent activities, the bank notified federal authorities, which led the FBI to arrest Hans Peter Walder on 24 September 2001. Walder was sentenced to 97 months (8 years) in prison in January 2003. He served his sentence in a federal prison in Ohio. After the incident UBS implemented a series of corrective actions to prevent similar occurrences. Policies were updated to include: call back procedures on disbursement of client funds; consolidated statements capturing all account activity; creation of retained mail analysis; clients were given internet access to view account history; all new loans required new documentation; and the principle of the four-eyed approach on disbursements was instituted. As a Private Banker, Walder was able to exploit his knowledge of the inner workings of the bank in order to defraud the institution by altering statements, capitalizing on hold mail policy, forging documents, allowing disbursement of funds without confirmations, abusing credit facilities on behalf of clients, etc. Initially, he believed that in purchasing the Castle he could turn a profit and pay back the loans he had obtained illegally. However, as the operational costs rose, the theft of client monies also rose.

Country: US
Key date: 2001 (UBS Private Banker arrested after defrauding clients and buying a Castle)

Tax Fraudsters - Tax Evaders

Mikhail Khodorkovsky

Mikhail Khodorkovsky was arrested at gunpoint on 25 October 2003, at a Siberian airport on charges of tax evasion, fraud, and theft. At the time of his arrest he was considered the most successful Russian Oligarch, the wealthiest man in the country by far and the 16th wealthiest in the world. Khodorkovsky's self-made fortune was estimated by Forbes to be approximately US\$15bio, mostly held through assets owned by the Menatep Group, chief amongst them OJSC Yukos Oil Company. Forbes now estimates that his personal wealth is approximately US\$500mio. His was not the first arrest. July 2003 saw the arrest of his

business partner Platon Leonidovich Lebedev, arguably Khodorkovsky's right-hand man. Lebedev (the second largest share holder in Yukos and a senior executive at the company) was arrested for fraud in relation to the 1994 privatisation of Apatit, a company engaged in the extraction of raw materials for the manufacture of chemicals and fertilizers. Lebedev's arrest may have been a warning specifically aimed at Khodorkovsky to leave Russia and to curtail his political gestures.

Many believe Khodorkovsky's woes stem from a personal vendetta against him by Putin, after the tycoon broke an unwritten pact between Russia's oligarchs and the Kremlin that they could keep their wealth as long as they stayed out of politics. However, rather than leaving Russia, Khodorkovsky entered into dialogue with Russia's regional governors and other politicians in order to persuade them to intervene – this perhaps angered Putin further. Khodorkovsky's arrest, like Lebedev's, related initially not to Yukos but to the privatisation of Apatit in 1994. A September 2011 report by the International Bar Association's Human Rights Institute²⁶ documents the criminal charges made against him by the government as being "[i]n 1994, while chairman of the board of the Menatep commercial bank in Moscow, M. B. Khodorkovsky created an organised group of individuals with the intention of taking control of the shares in Russian companies during the privatisation process through deceit and in the process of committing this crime managed the activities of this company". With respect to Apatit a state owned fertilizer manufacture, it was alleged that Khodorkovsky and his associates did not fulfill their investment obligations under the privatisation agreement, and that there was not a fair competitive bidding process for the 20% of Apatit that was being privatized in 1994. Allegedly the four companies that bid for the shares were front companies that ultimately were controlled by Khodorkovsky and Lebedev. Volna won the auction. Volna is a subsidiary company of Bank Menatep and it allegedly "misled" representatives of the administration of the Murmansk Region and members of Apatit's board by failing to adhere to the purchase agreement. The sale agreement required Volna to invest RUB563.17bio (US\$283mio) in developing Apatit and the town of Kirovsk over a period of two years. Apatit in return sued but the case did not go to court since the required funds were credited to Apatit's account held at Bank Menatep. However, apparently as soon as the case was settled the funds were transferred out of Apatit's account back to accounts under the control of Khodorkovsky. The 20% stake held by Volna was then sold to numerous companies all owned or controlled by Khodorkovsky and Lebedev. The "Khodorkovsky & Lebedev communication Centre" (a website developed

by the international legal team defending the two men) refutes these allegations and argues that the facts do not support the prosecutor's position. The Centre argues that had it not been for Khodorkovsky and his associates' investments and management, the company would not now be "one of the largest fertilizer producers in the world".

This was the first case against Khodorkovsky and Lebedev. The hearing lasted for two years and they were eventually imprisoned on May 2005 for eight years but with the possibility of early release. This prospect, however, was dashed when, in February 2007, new charges of embezzlement and money laundering were brought against both men. Also in 2003 the government made multiple claims against Yukos for failing to pay billions in taxes and made demands for repayment, ultimately this led to a Russian court in 2006 declaring the company bankrupt. Yukos' assets were sold off at bargain prices mostly to government owned entities. The fall of Yukos resulted in Khodorkovsky's own fortune falling to approximately US\$500mio. The second trial was concluded in December 2010 and the court found both Khodorkovsky and Lebedev guilty of embezzlement – stealing from Yukos and then laundering these proceeds. Prosecutors claimed they stole over US\$25bio of oil from the company over a period of several years – essentially, the entire output of the company. Commentators on the trial have highlighted concerns and in some cases laws were applied retrospectively to what were at the time commonly accepted business practices. Khodorkovsky's defence said that the second trial was a logical nonsense – in the first trial, he was convicted of tax evasion; and then he was accused of stealing the same oil he supposedly didn't pay tax on. A more cynical view is that figures in the Kremlin panicked that Khodorkovsky was due to be released in 2011 and scrambled to put together another case.

Khodorkovsky was, until a December 2013 pardon issued by President Putin, languishing in prison, but now he is released, surprising many including supporters, including international organisations such as Amnesty International, and many in political circles, who considered his incarceration to be politically motivated. While this view is furiously denied by the Kremlin, who would argue that the 2005 (and subsequent) trial of Khodorkovsky and associates was a just investigation based on merit, its critics argue that his imprisonment was an attempt by President Putin to silence a potential and credible presidential rival. Discussions on the fate of Khodorkovsky, his associates, and Yukos reached all levels in Russia but also around the world; from media and news to political pundits

and courtrooms; from local statesmen to the President of the US. Evidence of the discussions at political level and the debate that charges are politically motivated can be found in many places, including leaked US cables by WikiLeaks. For example, in a cable written in 2009 during the second trial against Khodorkovsky and Lebedev states that "[on] 23 December the Russian Supreme Court ruled that the 2003 decision to arrest and detain Lebedev was illegal, in keeping with a 2007 ruling by the European Court of Human Rights". The cables also argue that, while the second trial is apparently holding the rigors of fair legal proceeding, this in itself "may appear paradoxical" for a "case whose motivation is clearly political".²⁷

A number of NGOs and high ranking authorities campaigned to highlight the injustices of the case against the two men. For example, a report published by the Council of Europe in 2009 highlights the "authoritarian abuse of the system".²⁸ Statements of criticism can also be found from senior US administration officials including Hillary Clinton and various other US politicians. The same is true in the UK and other EU countries. Leading figures cite this case as the "erosion of democracy and rule of law in Russia". Sir Malcolm Rifkind, the former UK Foreign Secretary told the BBC "It is manifestly a politically inspired trial and Khodorkovsky is in effect a political prisoner". Khodorkovsky stated at the closing of the second trial, "Shameful. I am ashamed for my country."²⁹ With Khodorkovsky's release, Russia's most famous political prisoner is no longer behind bars. He has since his release, publicly announced he has no further interest in politics.

Country: Russia
Key date: 2003 (arrested by Russian authorities)

Operation Wickenby

Operation Wickenby is a code name adopted by the Australian Taxation Office and the Australian Crime Commission and a number of other Australian investigative agencies for the investigation into and prosecution of tax fraud and tax evasion. The probe commenced from data obtained from the computer of Philip Egginshaw a principal of Strachans Accountants. The computer was seized by a raid in his Melbourne hotel room in 2004, but has now moved to encompass a number of lines of enquiry and a broader probe and is not isolated to those parties associated with Strachans. The Strachans related investigations have been derived from advice to set up tax schemes which were marketed and promoted by both Egginshaw and another individual associated with the company, Philip de Figueiredo. Strachans initially operated from Jersey and thereafter Switzerland. As a result of the Australian prosecutions, De Figueiredo has since been arrested by

the Jersey authorities, however is yet to be extradited to Australia. As at September 2011, the Operation has secured 20 convictions which have led to imprisonment, and clawed back A\$1.18bio from parties associated with offshore accounts which were the proceeds of tax evasion. The cost of the Operation to date is estimated to be US\$300mio. The schemes used to achieve the evasion all contained the essential element in a tax fraud, that being dishonesty. The basic modus operandi of the schemes involved sending money to offshore companies based in secrecy havens that were controlled by Strachans, this money was disguised as loans. Strachans provided the perpetrators with credit or debit cards, some in fictitious names, enabling the proceeds to be withdrawn as cash, the intention being that such withdrawals would be untraceable.

While many of the existing cases remain sub judice, for the purposes of closer analysis, the case of Glenn Wheatley is worth a review. Glenn Wheatley has been an Australian music and entertainment manager and as part of his work in managing a successful tour of Australian entertainer Johnny Farnham, Wheatley was due to be paid as an employee of International Management Group of America Pty. Ltd ('IMG'). The conspiracy involved money that was due to be paid to Wheatley being directed to a Strachans associated company, the payment was not declared as assessable income by Wheatley. In a further fraudulent act, Wheatley was advised by his Australian practicing solicitor, Paul Gregory to divert his proportion of proceeds from a boxing match featuring Kosta Tszyu, being \$400,000 to a company called Overseas Promotions, this was also a company controlled by Strachans. Paul Gregory then assisted Wheatley embark on sophisticated deceit whereby Eggleinshaw would write to Wheatley with a false demand of \$700,000, Wheatley would respond to claim legal advice from Gregory was necessary and a pre-determined negotiated outcome would be reached for \$400,000. This deception was designed in order to assist Wheatley in avoiding paying tax. In relation to this particular offence, Wheatley plead guilty and received a 12 month sentence, Gregory, was sentenced to 16 months in imprisonment, a term which has been subsequently commented upon on appeal as being 'manifestly inadequate'. It is useful to analyse Wheatley's case as it involves the criminal participation of two gatekeepers of the anti-money laundering regime, lawyers and accountants. Their roles have been integral to the conspiracy. They had the intention to participate in the tax fraud. It appears with the success of recouping lost revenue, Operation Wickenby and its successors will run for some time still.

Country: Australia
Key date: 2004 (Australian authorities seize data from accountants computer that reveals hidden offshore accounts)

Pasquantino Brothers

Whilst in Niagara Falls, New York State, residents David

and Carl Pasquantino began smuggling cheap liquor from the US for sale on the black market in Canada in 1996. The brothers realised that Canada's average liquor tax was 83% and therefore was almost double that of the US. For over four years the Pasquantinos sourced liquor from discount stores in Maryland and hired drivers to avoid border controls by hiding liquor in their trucks. The smugglers, failed to declare it on Canadian customs forms and used US wires (phone calls) to place orders with the liquor stores in Maryland. Their activities cost the Canadian revenue almost US\$6mio. The Bureau of Alcohol Tobacco and Firearms investigating increases in orders into Maryland stores and with the stores co-operation finally gained evidence against the smugglers which led to their arrests. The smuggling of alcohol did not violate any US federal alcohol statute and although it did implicate an anti-smuggling statute, this one was unenforceable because there was no reciprocal agreement with Canada. Instead of extraditing them to Canada to stand trial on smuggling or fraud charges, the US authorities took a gamble and instead in April 2000 charged them with US Wire Fraud. They did this using a technicality to help shut down widespread liquor and cigarette smuggling between the US and Canada. In February 2001 a Maryland Federal court sentenced the brothers to five years in prison. The smugglers were convicted of wire fraud, that criminalises (1) "any scheme or artifice to defraud" combined with (1) use of the wires "for the purpose of executing such scheme." Defendants argued that their convictions should be reversed because (1) courts have recognised that a scheme to defraud must be aimed at depriving another of "property" and Canada's interests in collecting customs duties did not qualify, and (2) interpreting the wire fraud statute to apply to their conduct would contravene the common law revenue rule, pursuant to which US courts refuse to enforce another country's revenue laws. On appeal in 2002 this decision was reversed. Finally in April 2005, the Supreme Court, in a 5-4 decision, affirmed the brothers guilt on wire fraud based on a scheme to evade Canadian customs duties. In the current atmosphere of heightened scrutiny over financial transactions involving offshore clients, some have suggested that Pasquantino could criminalise certain conduct by non-US clients of US financial institutions and expand the obligations of such institutions to file suspicious activity reports ("SARs"). The Court, considering only the specific facts before it, rejected both arguments, explaining that Canada's interest in collecting taxes is "property" and that the revenue rule was not implicated because the wire fraud statute was punishing the defendants' US misconduct (i.e. misuse of US wires to help defraud others), not enforcing Canada's tax laws. In response to an argument made by dissenting justices, the Pasquantino majority held that it was not applying the wire fraud statute extra-territorially, because the scheme to defraud was conceived and completed in the US. Pasquantino does not expand the circumstances in which a US financial institution can be held criminally liable for a wire fraud scheme committed by one of its clients. A financial

institution itself should not commit wire fraud, unless it devises or actively participates in a scheme to defraud. A financial institution should not be liable as its client's co-conspirator, unless the institution agrees with the client to commit the wire fraud offense, and should not be liable for aiding and abetting its client's wire fraud, unless it intends to facilitate its client's wire fraud and assists or participates in the commission of the crime.

Pasquantino does not purport to change any of these standards. As a result, a financial institution's unknowing and unintentional involvement in a client's criminal activity is not unlawful. A US financial institution generally would not have any reason to know (or reasonably suspect) whether or not one of its non-US clients was honouring his or her home country tax obligations. Accordingly, absent knowledge or reasonable suspicion of a possible crime, the US financial institution should not violate any US criminal statute or reporting duty simply by virtue of the fact that a client wired monies into a bank as part of a client's scheme to avoid paying his or her tax obligations abroad. Pasquantino does not impose additional obligations on financial institutions to discover whether clients may be involved in criminal misconduct. Nevertheless, some have suggested that Pasquantino may require financial institutions to inquire whether their customers are satisfying their non-US tax obligations and, if the customer refuses to answer or the financial institution is not otherwise able to confirm that such tax obligations have been satisfied, the institution is required to file a SAR based on suspected fraud. No aspect of the Pasquantino decision directly supports this conclusion. Under the Bank Secrecy Act (the "BSA"), a US financial institution must file a SAR when it detects a known or suspected federal criminal violation transacted through the institution and exceeding certain monetary thresholds (e.g., \$5,000 for known, non-employee suspects). However, based on the Pasquantino decision, in the absence of a reasonable suspicion, a financial institution has no affirmative obligation, to inquire or attempt to discover whether such a violation has occurred, and absent knowledge or reasonable suspicion that a violation has occurred, the institution has no obligation to file a SAR. Further, if the client's conduct does not violate the wire fraud statute itself due to the particularities of this offence, the institution will not be obligated to file a SAR for that reason as well. Pasquantino's claim essentially that the US Government can't prosecute citizens for cheating the Canadians out of tax because of a long standing rule of law about not enforcing foreign tax laws was held to be invalid. Nevertheless, the above decision could be seen by some as expanding the application of the wire-fraud statute to cover foreign tax evasion, an expansion that could have consequences for businesses, tax cheats as well as bootleggers and as such arguably imports so called "all crimes" for this read "foreign tax evasion" as a predicate offense to money laundering.

Country: US, Canada

Key date: 2005 (US Supreme Court in a 5-4 decision upheld guilty verdicts for wire fraud based on evading foreign taxes)

Others

Douglas Jackson

Mr Jackson created a new business venture called E-Gold, registered in 1999 in Nevis in the West Indies which functioned as an alternative payment system and was purportedly backed by stored physical gold. Persons seeking to use the E-Gold payment system were only required to provide a valid E-Gold e-mail address to open an E-Gold account with no other contact information verified. Once an individual opened an E-Gold account, he/she could fund the account using any number of exchangers, which converted national currency into E-Gold. Once open and funded, account holders could access their accounts through the Internet and conduct anonymous transactions with other parties anywhere in the world. E-Gold claimed that the number of accounts grew from 1 million in November 2003 to 3 million in April 2006. In 2008, the company reported more than 5 million accounts.

The US government prosecuted resulting in 2008 guilty pleas from E-Gold, its founder and two senior directors accusing them of creating a vehicle which became a haven for criminals because of the anonymity E-Gold provided account holders, allowing cybercriminals to turn ill-gotten proceeds into clean cash. The indictment alleged that E-Gold has been a highly favoured method of payment by operators of investment scams, credit card and identity fraud, and sellers of online child pornography. The indictment further alleged that the defendants conducted funds transfers on behalf of their customers, knowing that the funds were the proceeds of unlawful activity; namely child exploitation, credit card fraud and wire (investment) fraud; and violated federal money laundering statutes.

The defendants were also charged with operating the E-Gold operation without the required licenses and thereby violated US federal and various state money transmitting laws. Law enforcement viewed E-Gold as a dangerous new threat that had the potential to be a favoured new banking channel. E-Gold was unique unlike previous digital currencies, E-Gold's focus on backing its accounts with gold provides more value than merely having money in a bank, especially in volatile markets. The judge found that whilst E-Gold was a haven for criminals, it was not the intent of Jackson to create such a business. Jackson was sentenced to 300 hours of community service, a US\$200 fine, and three years of supervision, including six months of electronically monitored home detention. E-Gold faced a maximum fine of US\$3.7mio, but they were fined US\$300,000. The defendants were also ordered to obtain licenses to do business in the states in which

a license is required for money transfer businesses. In September 2008, E-Gold hired KPMG to aid its development of an anti-money laundering programme.

Country: Nevis, US
Key date: 2008 (US prosecuted Jackson and others for money laundering offences)

PokerStars and Others

On 13 October 2006, the US enacted the Unlawful Internet Gambling Enforcement Act (UIGEA), making it a federal crime for gambling businesses to "knowingly accept" most forms of payment "in connection with the participation of another person in unlawful internet gambling." Shortly after the UIGEA was signed into law, Absolute Poker, an online poker company, announced that they would continue its US operation because "the US Congress has no control over" the company's payment transactions.

Despite the passage of UIGEA, the online poker companies, mostly those based in lightly regulated or unregulated jurisdictions in the Western Hemisphere, continued operating in the US. After the enactment of the UIGEA there was a temporary decline in online gambling by US residents, but the volume of online bets soon recovered. In fact the popularity of internet gambling continued despite the governments attempt to discourage it.

In 2010, online gambling revenues from US gamblers exceeded US\$4bio.

On 15 April 2011 the US government announced indictments against 11 individuals. Seven of the defendants are the poker companies; PokerStars, Full Tilt Poker, and Absolute Poker ("Poker Companies") and their owners and executives, and the remaining four are their payment processors, including one banker. The charges included money laundering, bank fraud and illegal gambling offenses, with the focus on the processing of payments to and from the gambling websites' customers, in contravention of the Unlawful Internet Gambling Enforcement Act. The US government also filed a civil money laundering and forfeiture case against the Poker Companies, their assets, and the assets of several payment processors for the Poker Companies. The indictment alleged that the online operators tricked banks into processing billions of dollars in payments from customers. In one instance, after US banks and financial institutions detected and shutdown multiple fraudulent bank accounts used by the betting websites in late 2009, the founders developed a new processing strategy. For example, one of the payment processing companies, created fictitious companies, including fraudulent online flower shops and pet supply stores, to help facilitate credit card transactions, to have developed pre-paid debit cards or phone cards that could be loaded with funds from a US customer's credit card without using a gambling transaction code. Of the billions in dollars in payment

transactions that the poker companies tricked the US banks into processing, about one-third of the funds went directly to the poker companies as revenue.

The US Department of Justice seized the .com internet addresses of the three online gambling sites, replacing them with a takedown notice, but let Full Tilt and PokerStars use them again once they pledged to no longer serve the US. About 76 bank accounts in 14 countries were frozen, including an unknown amount of player funds. The prosecutors sought jail sentences for the 11 criminal defendants including site founders and executives, US payment processors, and an executive of a small Utah bank, who prosecutors maintain were engaged in an elaborate criminal fraud scheme, using the bank in Utah to mis-code transactions with other banks to bypass UIGEA restrictions. The companies ceased their U.S.-facing ad campaigns, resulting in cancellations of poker-themed television shows. In June, Full Tilt had its e-Gambling license suspended, which halted all of its remaining online play. The Alderney Gambling Control Commission on the British Channel Islands later revoked its license. In July 2012, the US government dismissed "with prejudice" all civil complaints against all PokerStars and Full Tilt Poker companies after coming to a settlement with PokerStars which includes PokerStars purchasing Full Tilt and agreeing to pay US\$731mio. Nevertheless, the criminal indictments remain in place for the named individuals.

Whilst many of those indicted were beyond the direct jurisdiction of US authorities, one of the payment processors, Ira Rubin was not, and he pleaded guilty to conspiracy charges related to illegal gambling, bank fraud, wire fraud, and money laundering on behalf of three online gaming sites and was sentenced to three years in prison. Absolute Poker co-founder Brent Buckley pled guilty to misleading banks, and he was sentenced to 14 months. John Campos was part-owner and vice chairman of the board of directors for SunFirst Bank, who pled guilty to a single misdemeanor bank gambling charge, being sentenced to three months in prison. During his plea, Campos said his processing of the gambling proceeds for PokerStars and Full Tilt Poker was not in return for a US\$10 million investment in the bank.

Insider Traders

R Foster Winans

Winans was a former columnist for The Wall Street Journal who co-wrote the "Heard on the Street Column" from 1982 to 1984 and was convicted of insider trading and mail fraud. He was indicted by then-US Attorney Rudolph Giuliani and convicted in 1985 for leaking advance word of the contents of his columns to a stockbroker, Peter N. Brant at Kidder, Peabody & Co. Winans' conviction was affirmed by

the US Supreme Court in 1987 as *Carpenter v. US* by a rare 4-4 deadlocked vote. Winans admitted his participation in the scheme and to earning US\$31,000 from it, but pleaded not guilty, arguing that his behavior was unethical but not criminal. Winans was found guilty and sentenced to 18 months in prison, serving 9 months. Both the securities industry and the First Amendment lobby criticized the prosecution as over-stepping the bounds of the securities laws, and filed amicus briefs during the appeals process. Winans' case included two co-defendants and reached the US Supreme Court in 1987. The missing member was due to the retirement of Justice Lewis F. Powell, Jr. The US Supreme Court cited an earlier ruling while unanimously upholding mail and wire fraud convictions for a defendant who received his information from a journalist rather than from the company itself. R. Foster Winans conviction was also upheld on the grounds that he had misappropriated information belonging to his employer, the Wall Street Journal. The court ruled that "It is well established, as a general proposition, that a person who acquires special knowledge or information by virtue of a confidential or fiduciary relationship with another is not free to exploit that knowledge or information for his own personal benefit but must account to his principal for any profits derived therefrom." Winans once observed: "The only reason to invest in the market is because you think you know something others don't."

Country: US

Key date: 1985 (convicted of insider dealing for leaking advance word of his newspaper column "the heard on the street" to his broker)

Special Focus 15 Ivan Boesky & Others



The son of a Russian immigrant, Ivan Boesky started on Wall Street in 1966 as a stock analyst. Marrying into money, helped Boesky start his own arbitrage firm in 1975. By the mid-Eighties, "Ivan the Terrible" as he became known was worth an estimated US\$200mio, through trading in stocks of companies targeted for takeovers. Corporate mergers and acquisitions soared in the 1980s. Nearly 3,000 mergers and buyouts worth more than US\$130bio

occurred in 1986 alone, many of these takeovers taking the form of leveraged buy outs, financed from junk bonds, many of which were arranged by Michael Milken and the firm in which he was the star banker, and undisputed junk bond king, Drexel Burnham Lambert.

Using a fund established by limited partners, Boesky would bet on takeover situations, mostly after a deal had already been announced, making a profit if the deal went through at the announced price, but losing money if the deal fell through. In May 1982, Gulf Oil announced a takeover attempt of Cities Service but the takeover failed. Boesky had placed a large bet that the takeover would go through, losing around US\$24mio on this deal. It was this loss, it is believed, that led Ivan to conclude that he needed a greater edge and so he began to build a secret network of investment bankers and brokers who would then supply him with insider information and in return would receive a cut of the illegal profits. Two of the key figures in this network were Martin Siegel of Kidder Peabody and Dennis Levine of Drexel Burnham Lambert.

Using inside information supplied by Siegel, Boesky made US\$28mio from Nestle's acquisition of Carnation in 1984 and up to US\$50mio on further tips from Mr Siegel. In return Boesky paid Seigel between 1 to 5% of the profits made and in one case paid him US\$800,000 in cash. In one case Levine made US\$2.69mio. Boesky was successful making lots of money on many of the major takeover deals in the 1980s, for example, Getty Oil, Nabisco, Chevron and Texaco profiting from insider tips. Despite these repeat successes, defying the odds, and as was becoming common, the share prices of stocks in companies targeted for leverage buyout (LBO) or hostile takeovers would rise before the deals were announced, indicating that insider trading was occurring, the SEC took no action. It wasn't until Merrill Lynch provided the SEC with their own inside tip that the SEC would start an investigation that would lead to the arrest of first Dennis Levine of Drexel Burnham Lambert, and then Ivan Boesky and Martin Siegel.

Levine spent most of his career as a specialist in mergers and acquisitions. He was known as a good researcher with a voracious appetite for information. Over the years, Levine built up a network of professionals at various Wall Street firms who engaged in insider trading. Participants exchanged and traded on inside information they obtained through their work. Levine placed his trades through an account maintained firstly at Bahamian subsidiaries of Swiss banks, Pictet & Cie, and then at Bank Leu eventually earning more than US\$10mio in profits. Some of those at Bank

Leu realized that Levine must have been trading on inside information and instead of shutting down the account and informing the authorities, some of them decided to copy Levine's trades, known as "piggyback trading", making money themselves. In order to protect Levine's trading from discovery, Bank Leu traders broke up Levine's trades among several brokers. A broker at Merrill Lynch, also began piggybacking the trades for himself. In May 1985, Merrill Lynch detected suspicious activity in two brokers' personal trading accounts, which led an internal investigation to focus on the trades coming from Bank Leu in the Bahamas.

Unable to get information on the client at Bank Leu, due to Bank Leu's resistance and Bahamian banking secrecy, Merrill Lynch informed the US Securities and Exchange Commission (SEC). The SEC aggressively pursued Bank Leu, who would ultimately co-operate but not after destroying many documents related to Levine's activity. Their retained lawyer, Harvey Pitt (a future SEC head) had noted major discrepancies in their answers to his questions and he insisted that they come clean. Bahamian Attorney General Paul Adderly issued an opinion that stock trading was separate from normal banking transactions, and thus was not subject to the bank secrecy laws. The bank was thus free to reveal Levine's name, and he was arrested soon afterward.

On 5 June 1986, Levine pleaded guilty to securities fraud, tax evasion and perjury. He also agreed to cooperate with the government and revealed the other members of his insider trading ring. Levine also settled the SEC's charges, agreeing to disgorge US\$11.5mio—at the time, the largest such penalty in SEC history. He also agreed to a lifetime ban from the securities industry. Levine also agreed to pay US\$2mio in back taxes out of the amount he disgorge to the SEC. Subsequently, Levine directly implicated Ivan Boesky, and information from the Boesky case also implicated Martin Siegel. Both Boesky and Siegel subsequently pleaded guilty. The investigations also led to [Michael Milken](#), who was highly influential in the junk bond market at the time.

Due in part to his cooperation, the judge imposed a lenient sentence of two years in prison and a US\$362,000 fine on Levine. Boesky admitted to numerous offenses and then turned state's evidence, primarily against Milken. He received a 3 1/2 year prison sentence (of which he served 18 months) and US\$100mio fine after admitting to the charges, reaching a very favourable plea bargain with Rudy Giuliani, US attorney for the Southern District of NY. The authorities even allowed Boesky to reduce his partnership liabilities by selling stocks and securities before his crimes were made public. In return for

leniency, Boesky allowed the SEC to secretly tape his conversations with associates. The prize sought though was Michael Milken. Boesky lured Milken to a hotel room, where they discussed deals in a conversation recorded using a microphone hidden in Boesky's clothes.

The case against Milken was not clear cut however. For more details see [Michael Milken](#) later.

As Boesky left federal court in 1987 to serve his sentence he proclaimed, "Greed is all right...everybody should be a little greedy." The invocation of greed, was a throwback to a famous quote from Boesky in 1985 telling an audience of business students at Berkeley, that "Greed is all right, by the way—I want you to know that," and that "I think greed is healthy. You can be greedy and still feel good about yourself." The greedy Boesky also admitted in an interview that he fantasized about climbing atop a huge pile of silver dollars: "Imagine—wouldn't that be an aphrodisiac experience?"

Boesky's story inspired the 1987 movie "Wall Street," with Michael Douglas playing a reptilian character named Gordon Gekko—who recited, nearly word for word, Boesky's now-legendary "greed is good" speech.

Penalty: US\$100mio fine and imprisonment

Actions: Insider dealing, implicating others and helping to bring down Drexel Burnham Lambert and Michael Milken

Country: US, Bahamas

Key date: 1987 (found guilty of insider dealing charges)

George Soros

In 1988 Soros was interested in purchasing shares in French companies. The Socialist Party had lost its majority of seats in the Assembly and the new government under President Chirac had instituted an aggressive privatisation programme. Many people considered shares in the newly privatized companies undervalued. During this period, a French financier named Georges Pébereau contacted one of Soros' advisors in an effort to assemble a group of investors to purchase a large amount of shares in Soc Gen, a leading French bank that was part of the programme. The advisor reported to Soros that Pébereau's plan was ambiguous and included an implausible takeover plan (it would indeed fail). On that advice, and without ever meeting the financier, Soros decided against participating. He did, however, move forward with his strategy of accumulating shares in four French companies: Société Générale, as well as Suez, Paribas and the Compagnie Générale d'Électricité. In 1989,

the Commission des Opérations de Bourse (the French stock exchange regulatory authority) conducted an investigation of whether Soros' transaction in Société Générale should be considered insider trading. Soros had received no information from Société Générale, and had no insider knowledge of the business, but he did possess knowledge that a group of investors was planning a takeover attempt. The COB concluded that the statutes, regulations and case law relating to insider trading did not clearly establish that a crime had occurred, and that no charges should be brought against Soros. Several years later, a Paris-based prosecutor reopened the case against Soros and two other French businessmen, disregarding the COB's findings. This resulted in Soros' 2005 conviction for insider trading by the Court of Appeals (he was the only one of the three to receive a conviction). The French Supreme Court confirmed the conviction on 14 June 2006, but reduced the penalty to the minimum. Punitive damages were not sought because of the delay in bringing the case to trial. Soros denied any wrongdoing, saying news of the takeover was public knowledge and it was documented that his intent to acquire shares of the company predated his own awareness of the takeover. In December 2006, he appealed to the European Court of Human Rights on various grounds including that the 14-year delay in bringing the case to trial precluded a fair hearing. On the basis of Article 7 of the European convention on human rights, stating that no person may be punished for an act that was not a criminal offence at the time that it was committed, the Court agreed to hear the appeal. In October 2011, the court rejected his appeal in a 4–3 decision, saying that Soros has been aware of the risk of breaking insider trading laws.

Country: France

Key date: 1989 (French regulators start investigation into insider dealing)

Special Focus 16

Ernest Saunders



Ernest Saunders had a career in management with Beecham, Great Universal Stores and Nestlé before becoming Chief Executive and Chairman of Guinness Plc (now a part of Diageo Plc) in 1981, remaining in the position until 1986 on a salary of £375,000pa.

He was born Ernest Walter Schleyer in Austria and moved to the UK in 1938 when his parents emigrated to escape Nazi rule. He was renowned for his ambition and ruthless cost-cutting efficiency, earning from his employees the nickname 'Deadly Ernest'.

He would however become best known as one of the "Guinness Four", a group of businessmen who attempted to fraudulently manipulate the share price of the Guinness company. He was sentenced to five years' imprisonment, but released after 10 months as he was suffering with apparent Alzheimer's Disease. After leaving prison he fully recovered.

Determined to turn a brewer of unfashionable stout as well as a collection of more than 150 other businesses ranging from sweets to canal boat holidays, into a dynamic, international drinks conglomerate, Ernest Saunders quickly 'rationalised' - cutting down, selling off and closing up parts of the business. He ditched the Guinness campaign in favour of the Genius campaign. Profits and the share price went up. But there was a limit to rationalisation and so next he focussed on growth by acquisitions. Saunders, flexed his muscles on buying a chain of newsagents and then took over the Arthur Bell, the Scotch group in an acrimonious bid battle. He then identified "Distillers" which owned whisky brands such as Dewars and Johnnie Walker and in 1986 when Distillers became the subject of a hostile bid from Argyll, a retailing group, Saunders saw his chance.

Saunders, in secret talks with Distillers, secured their approval for a friendly merger, with Guinness agreeing to pay for Distillers by a combination of cash and shares. At the start of the bidding war Argyll looked set to win as the Guinness share price stood at around 280p a share and as such valued Distillers at around £2bio. Within weeks however, Guinness shares rose to a peak of 353p, which valued Distillers at £2.5bio and allowed Guinness to win the bidding war.

At the time, the sudden share surge seemed to reflect shareholder confidence and support for the acquisition. It wasn't until later that SEC investigators would provide information to their UK counterparts that the truth behind the surge would become known. The tip came from none other than [Ivan Boesky](#), who was co-operating with US authorities and in a plea bargain, provided the critical information that led to the share support operation being exposed. [Ivan Boesky](#), on whom Gordon Gekko from Wall Street fame was based, told US authorities that a friend of Ernest Saunders, Gerald Ronson first contacted him about the Distillers bid soliciting his support to purchase Guinness shares

in early 1986, and assured him that Guinness would "repay any losses" incurred. These terms were confirmed with a non-executive director of Guinness. The terms would also include a monthly kickback fee of 5% on any sums invested.

With these assurances in place Boesky began to build up his position ultimately holding 14 million Guinness shares at a cost of about US\$80mio, by the time the bid became successful. In addition to mobilising Boesky, Guinness used friends to 'support' and push up the share price. Methods ranged from indemnities and guarantees on losses and also included the illegal purchase of its own shares. At the same time, Guinness was driving down the value of Argyll shares.

Following the tip from America and after an investigation into the allegations by UK inspectors, Saunders (along with others including 3 leading UK entrepreneurs, Jack Lyons, Anthony Parnes and Gerald Ronson) was prosecuted and convicted in 1990 of fraud in operating an illegal share support operation so as to keep the Guinness share price attractive to Distillers shareholders and ensure a Guinness victory.

Mr Saunders claimed he knew nothing of these illegal arrangements. At his trial in 1990, the judge and jury found otherwise. However, Saunders was released just over nine months into his five year jail sentence, after producing a medical report which said that he might be suffering from the early onset of Alzheimer's Disease. He quickly made a remarkable recovery. Ronson was sentenced to one year in prison and given the then biggest fine in British history, US\$9.75mio (£5mio), for what the judge called "an attack on the integrity of the market."

Country: UK
Key date: 1990 (prosecutions and convictions in UK's biggest Insider Trading case)

James McDermott Jr
The former chairman and CEO of Wall Street investment bank Keefe, Bruyette & Woods Inc. (KBW), was charged in 1999 and convicted of insider trading for passing inside information to his girlfriend, porn actress Kathryn B. Gannon, also known as "Marylin Star." McDermott passed insider secrets to Gannon, who then told another boyfriend, Anthony Pomponio. McDermott did not act on the information, but Gannon and Pomponio each made more than US\$80,000. McDermott was barred from working in the industry and served five months in prison. Gannon and Pomponio each served three months.

Country: US

Key date: 1999 (charged with insider dealing and convicted and imprisoned for 5 months in US)

Martha Stewart

About an hour after the verdict was read, Stewart - wearing a fur around her neck and a black overcoat and carrying a brown leather bag - strode poker-faced down the stairs of the courthouse, accompanied by her lawyers, and left. She did not respond to questions shouted at her by reporters. As she came within sight of a crowd in the street, some people began chanting, "We want Martha!" The above is how CNNMoney reported Martha Stewart's exit from court following her conviction on four charges relating to a well timed stock sale. Born in 1941 Martha Stewart is a household name in the US and across the world. Stewart started her career in the investment industry after passing her broker's exam in 1968 and spent 5 years on Wall Street. After this short spell on Wall Street she launched her catering business and her first book 'Entertaining' was published in 1982. Magazine deals, endorsements followed and then in 1993 her own weekly TV show 'Martha Stewart Living' was launched. Her business Martha Stewart Omnimedia was publicly listed on the NYSE in 1999. So how did this modern day 'Mrs Beeton' find herself at the centre of a media circus, a criminal trial and subsequent imprisonment?

The charges against Stewart related to an incident that occurred on 27 December 2001 when Peter Bacanovic, her broker at Merrill Lynch, ordered his assistant to tell Stewart that the ImClone CEO Samuel Waksal, his family and friends were selling shares in advance of a negative ruling by the Food and Drug Administration. Upon receipt of this information Stewart sold her entire holding of nearly 4,000 ImClone shares. The next day the FDA announced its ruling which rejected ImClone's application for a licence for a cancer drug. As a result, ImClone's shares fell by 16% during trading on the day of the incident. Stewart's prescient sale allowed her to avoid a loss of US\$45,000. In June 2002 Samuel Waksal was arrested after it was established that his family and friends and also other company executives had sold over US\$15mio worth of shares prior to the announcement. Waksal would later be sentenced on this and other conspiracy, wire fraud and tax charges to over seven years in jail and more than US\$4mio in fines and back taxes.

With the spotlight on ImClone trading it is no surprise that a review of similarly timed trading was undertaken and Stewart became embroiled in the scandal. Stewart repeatedly denied any wrong doing stating that the stock sale was based on an early price agreement with

her broker. Her position was subsequently weakened after Merrill Lynch suspended Bacanovic on 21 June 2002 after an internal investigation identified conflicting accounts about whether Stewart's sale price agreement with Merrill Lynch existed. In September 2002 a House committee asked the Department Of Justice to launch an investigation into Stewart's alleged insider dealing. This investigation initially forced Stewart to step down from the NYSE board to which she had recently been appointed and later from the board of Martha Stewart Omnimedia. The investigation highlighted sufficient evidence to bring a case against Stewart who was to stand trial in March 2004. Throughout the investigation Stewart continued to deny the allegations and came to trial with a phalanx of lawyers. The prosecution reacted in kind. Because of Stewart's fame the court proceedings became a show trial for the five weeks it ran, with wall to wall TV coverage and acres of column inches devoted to the case. This made it the most talked about corporate fraud cases of that period. This provided the prosecution with the perfect opportunity to demonstrate that they were prepared to bring cases against famous individuals and that no one was above the law because of their fame or connections.

The five week trial ultimately established that both Stewart and Bacanovic were guilty of conspiracy, obstruction of agency proceeding and making false statements to federal investigators in relation to the ImClone investigation. It is important to highlight that Stewart was not tried for insider dealing. If she had admitted when first approached by the Department of Justice/Regulators that she had acted upon the information received from Bacanovic then in all likelihood she would have been able to plea-bargain and probably only faced a fine. However, as she denied the allegation throughout, she was not able to benefit from a bargain and once convicted faced the full consequences of her actions and her earlier efforts to obstruct the investigation.

Her sentence was delivered in July 2004. Stewart was only given the minimum punishment available; she was required to spend five months in prison, a further 5 months under house arrest and to pay a fine of US\$30,000. Although this brought to an end the criminal proceedings against her, Stewart also had to settle the civil insider dealing charges with the SEC. An out of court settlement was reached in August 2006 where Stewart agreed to pay US\$195,000, (US\$58,000 in disgorgement and US\$137,000 in civil penalty). She was also barred from serving as a director of chief executive officer of any public company for five years. Ultimately, the advice Stewart received to sell shares

which initially saved her US\$45,000 ended up costing her far more and included a period of incarceration, disgorgement and fines totalling US\$225,000, extensive legal costs and damage to her reputation, company and brand including lower profits necessitating the loss of staff. Remarkably Stewart has been able to rebuild her company and a quick Google search identifies that her brand goes from strength to strength. Maybe this is as a result of the fact that insider dealing is, by some, still often seen as a victimless crime. Fans have therefore been able to continue to support her in a way they wouldn't have been able to if she had committed what the public might consider a less palatable offence.

Country: US

Key date: 2002 (US Congressional Committee requested investigation into Stewart's alleged insider dealing)

Philippe Jabre

Mr Philippe Jabre and GLG Partners LP (GLG) were each fined £750,000 for market abuse and breaching UK Regulator's principles. On 11 February 2003 Mr Jabre a former managing director of GLG was 'wall crossed' by Goldman Sachs International as part of the pre-marketing of a new issue of convertible preference shares in Sumitomo Mitsui Financial Group Inc (SMFG). Mr Jabre was given confidential information and agreed to be restricted from dealing SMFG securities until the issue was announced. Mr Jabre breached this restriction by short selling around US\$16mio of SMFG ordinary shares on 12-14 February 2003. When the new issue was announced on 17 February 2003, Mr Jabre made a substantial profit for the GLG Market Neutral Fund. Margaret Cole, FSA Director of Enforcement said: "Mr Jabre traded on information he had received as a result of the position he enjoyed as a leading hedge fund manager. The stability and fair operation of the markets through legitimate pre-marketing activities is jeopardised if those who are wall-crossed do not respect the restrictions imposed on them. "GLG is also responsible for Mr Jabre's market abuse. Firms are accountable for the behaviour of their employees, particularly if they are at a senior level."³⁰

Country: UK

Key date: 2003 (investigations started into insider dealing of hedge fund manager)

Anthony Elgindy & Others

Elgindy paid an FBI Agent Jeffrey Royer, to log into government databases using his credentials to dig up confidential information that could then be used for financial gain. For instance, if the CEO of a company

had an ongoing criminal investigation against him, Elgindy would short the stock (bet that it would fall) and then disseminate the confidential information which would usually trigger a fall in prices. Elgindy would also inform the companies that he possessed this information, and then try to extort funds from them in exchange for not releasing the info. Eventually the FBI caught on to the scheme and Elgindy ended up receiving 11 years in jail.

Country: US
Key date: 2005 (convicted of insider dealing)

Michael Guttenberg & Others

Michael Guttenberg, an institutional client manager in UBS' equity research department in New York was arrested and sentenced in 2006 to six and a half-years in prison and ordered to pay back US\$15.8mio he made from his involvement in an insider trading scheme involving several hedge funds. Guttenberg had access to potentially price sensitive confidential information due to his membership on the UBS's Equities investment review committee since 2001. As a member of this Committee, Guttenberg regularly had access to stock recommendations by influential UBS analysts before the information was made public. Guttenberg provided this information to two Wall Street traders, for example a 2006 downgrade of Caterpillar Inc., the world's largest maker of bulldozers, and a 2006 upgrade of Goldman Sachs Group to Erik Franklin and David Tavyd, in exchange for a cut in the profits they made from trading on that information.

Erik Franklin and David Tavyd in turn cut more deals and gave tips to others who made money on this information. He also passed hundreds of tips to Tavyd and Franklin. At a meeting at the Oyster Bar in New York's Grand Central Station in 2001, Guttenberg offered to settle a US\$25,000 debt to his friend Franklin, by slipping him analyst ratings in advance. At the time, Franklin was working at Bear Stearns in New York and managing money for Lyford Cay Capital, which invested on behalf of some of Bear Stearns' senior officials. He and his colleague, David Tavyd made more than US\$4mio on inside trades in brokerage accounts they controlled. Three Bear Stearns brokers also traded on Guttenberg's tips. He continued to do this from 2001 to 2006 and was paid hundreds of thousands of dollars, while others who were involved in this insider trading made more than US\$17.5mio. Guttenberg made similar deals with others, including another hedge-fund manager where he routinely provided tips about ratings changes on stocks such as Amgen Corp, Whole Foods Market, and Union Pacific Corp. He tried to cover his tracks by using coded text messages made from disposable cell phones, no use of e-mails, no telephone calls, no trading in his personal account, no wire transfers accepting only cash.

In a separate but connected scheme, Randi Collotta was working as a compliance officer for Morgan

Stanley in New York. Collotta worked with her husband a New York Attorney to leak price sensitive information to her friend Marc Jurman, a broker in Florida, and others for example in 2004 and 2005 information about Johnson & Johnson's failed US\$24.2bio bid for Guidant Corp, UnitedHealth Group Inc's US\$8.2bio acquisition of PacifiCare Health Systems Inc. and ProLogis' US\$5.5bio purchase of Catellus Development Corp were leaked. In addition to Marc Jurman, the information was sold to Wall Street hedge fund traders including Erik Franklin at Bear Stearns. As an active Hedge Fund trader, Franklin thought he could bury these trades in the mass of trading conducted on the exchange and via his 50 to 100 different trades per day. The demand for performance among hedge funds where a percentage point in performance can mean the difference in millions of dollars of additional compensation based on pre agreed performance fees is a clear risk factor.

It appears that the SEC was able to pick up irregular profitable trading patterns in the merger and acquisition of two publicly traded companies, Adobe Systems, and its acquisition of Macromedia in 2005, and ProLogis, and its acquisition of Catellus Development. Once the SEC saw the irregular trading, they then focussed on those trading ahead of publicly available information, then matched these professional investors with other public deals to identify whether similar patters could be identified. Randi and Christopher Collotta was sentenced to four years' probation and three years' probation respectively. None of the Wall Street firms were named in the criminal or civil complaints. Linda Thomsen, the SEC's then enforcement chief, described the trading scandal as "one of the most pervasive Wall Street insider trading cases since the days of Ivan Boesky and Dennis Levine."

Franklin pleaded guilty to two counts of conspiracy, securities fraud and commercial bribery in February 2007. Erik Franklin co-operated with the authorities, ultimately sentenced to 3 years probation. He was also ordered to forfeit US\$2.59mio and to complete 200 hours of community service. Franklin's co-operation led authorities to another trader David Slaine and he in turn pleaded guilty and told the authorities about the activities of Zvi Goffer. Goffer, a former Galleon Group employee, was arrested in November 2009 and accused of leading an insider-trading ring tied to the Raj Rajaratnam investigation. Tavyd by contrast had little to offer the authorities in a plea bargain and was sentenced to 63 months in prison.

Country: US
Key Date: 2006 (arrested and convicted of insider dealing)

Takafumi Horie

In Japan, the case of Livedoor Co, in 2006, was one of the biggest insider trading scandals which engulfed the flamboyant former president of the Internet

company and shareholder activist in legal flames. The case goes back to July 2003 when Yoshiaki Murakami, a former investment manager, and his Murakami Fund emerged as the second-biggest shareholder in Nippon Broadcasting. Mr. Murakami later raised the fund's stake in the radio station to become the largest shareholder – and unbeknownst to him, laid the plot elements for the attempted hostile takeover bid that would come back to bite him three years later. In May 2004, the Tokyo-based Nippon Broadcasting rejected Murakami's overtures to become an outside member of its board. That allegedly then led to collusion between the financier, Murakami and Takafumi Horie, the ex-president of Livedoor. On 15 September, Mr. Murakami allegedly urged Livedoor, an Internet and financial services company, to purchase Nippon Broadcasting shares with the aim to gain control over the Fujisankei Communications Group. On 8 November Mr Murakami reportedly obtained information from Livedoor's top management that the start-up company planned to buy a large amount of shares in Nippon Broadcasting. The following day the Murakami Fund started to purchase additional shares of the radio station. During their subsequent trials, both men said the purchases were a coincidence. Livedoor announced it acquired a 35% stake in the radio station on 8 February and it was believed that the Murakami Fund had sold a slice of its shareholding to the company. On 5 June 2006 the day Mr Murakami was arrested. Prosecutors asserted that the Murakami Fund acquired 1.93 million shares in the radio broadcaster between November 2004 and January 2005, acting on the non-public information from Livedoor that it was trying to grab a 5% stake in the business. The investment fund earned about JPY3bio (US\$25.5mio) by selling about 5 million Nippon Broadcasting shares to Livedoor. Mr Murakami narrowly avoided a prison term. The Tokyo High Court overturned a lower court ruling that sentenced the ex-fund manager to two years in jail, revising it to a suspended term for three years in February 2009. But Mr. Murakami was still forced to pay a JPY3mio fine and a JPY1.15bi in additional penalties. The former Livedoor leader was not as lucky. In March 2007, Mr. Horie, the rebellious internet entrepreneur that favored casual dress over business suits, was convicted and sentenced to two and a half years in jail for his role in a securities fraud.

Country: Japan
Key date: 2006 (arrested and charged with insider dealing in connection with Japan's first hostile takeover bid)

Chen Rongsheng

Chen Rongshen, a chinese businessman who started by cultivating and selling mushrooms, then exporting eel snacks to Japan, became in 1999 the first private company from Xiamen province to list on the Shanghai Stock Exchange changing its name on listing Xiamen Prosolar Technology. Chen controlled the company

indirectly, owning much of the company shares. The company continued to prosper and its shares increased in value, for example Xiamen Prosolar's profits jumped to 110 million yuan in 2007 after the company sold a real estate project subsidiary. Chen, along with company executives then sought advice from a securities firm about a plan to inject assets into Xiamen Prosolar in April 2007. A deal was reached a month later. But this information was only released to the public some time later. In the meantime and during the time Chan had inside information he bought shares in Xiamen Prosolar in the secondary market. Investigators found that, Chen opened a few hundred different broking accounts via various parties with Chen having the ultimate authority. Later, in 2007, Chen successively transferred about 50 million yuan from Dragon Wing and Shanghai Zhen to numerous securities accounts opened by these companies, which then traded in Xiamen Prosolar stock. Astonishingly Chen may have made up to 19 billion yuan in all (US\$3bio) through insider trading in Xiamen Prosolar stock. This was the first insider dealing case in China according to the China Securities Regulatory Commission (CSRC). Chen transferred most of his assets to his 24-year-old son, Chen Guanquan, in 2008. A year later, the young man was on the Hurun List of Richest Chinese men. Chen was arrested and prosecuted and sentenced to two years in prison with a two-year reprieve.

Country: China
Key date: 2007 (China's first insider dealing case, led to Chen's arrest and imprisonment of 2 years)

Chris Littlewood & Others

Chris Littlewood, his wife, and family friend Helmy Omar Sa'aid all pleaded guilty to insider dealing on the London Stock Exchange and AIM listed shares. Littlewood, who earned £350,000 a year working for German investment bank Dresdner Kleinwort Wasserstein with access to inside information.

Littlewood passed information to his wife who then passed this on to family friend Helmy Omar Sa'aid. The FSA investigation began in August 2008 when a standard review of trading patterns ahead of the announcement of a possible takeover of a company revealed that Mr Sa'aid regularly bought a small number of shares in the company in the weeks before the announcement. Further investigation of Mr Sa'aid's trading activities revealed that he had made similar trades before 22 other merger announcements. The FSA checked and learned that one Bank had advised on 15 of those 22 deals, and therefore this was most likely the source of the inside information. The breakthrough in the investigation which tied Mr Sa'aid to Mr Littlewood came when the FSA checked Mr Sa'aid's bank accounts and found that a Ms Siew Yoon Lew paid money from her bank account into the account of

both men. Siew Yoon Lew was the maiden name of Mr Littlewood's wife. Ms Lew was the conduit by which the insider dealing was conducted. Her husband passed information to her which she then made available to Mr Sa'aid, and after the deal had been made payment was facilitated through her bank account.

Littlewood was sentenced to three years and four months in custody, Sa'aid to two years and Mrs Littlewood to twelve months, suspended for two years. Littlewood, 37, spied on colleagues to pass on information so that he and his wife Angie, 39, and her friend Helmy Sa'aid, 34, could make almost £600,000, on investments of £2mio on LSE shares purchased between 2000 - 2008 in what the judge described as "the biggest prosecution for insider trading ever brought".

Country: UK
Key date: 2008 (investigations into insider dealing started by UK FSA)

Nicos Stephanou & Others

On 27 December 2008, when his Cancun-to-London flight stopped at Newark Liberty International Airport, Greek Cypriot, Nicos Stephanou was arrested on insider dealing charges.

Stephanou had joined UBS in 2002 after working in the corporate finance department of Coopers & Lybrand LLP and the mergers and acquisitions group at Credit Suisse. Whilst at Credit Suisse in London, Stephanou became friends with Ramesh Chakrapani who later moved to the Blackstone group. In 2006, Nicos Stephanou was a member of the team at UBS that advised ABS on its response to an approach by a consortium of buyers looking to acquire the company, prior to ABS publicly announcing that this approach would lead to an agreed takeover. Also in 2006, ELK publicly announced that it had agreed to be acquired by The Carlyle Group. ELK hired UBS as its financial advisor. Nicos Stephanou also worked on this deal. In late 2006, NHI publicly announced that it had retained Blackstone as its financial adviser to consider strategic alternatives and had received a buyout offer from its CEO, but stated that the offer was inadequate. Ramesh Chakrapani as an employee of Blackstone had access to material non-public information concerning this announcement by virtue of his membership of the team at Blackstone that advised NHI on strategic choices. Ramesh Chakrapani and Nicos Stephanou each provided inside information they were privy too, to family members and to Joseph Contorinis, a hedge fund trader and personal friend at Jefferies Group. Nicles Stephanou and Ramesh Chakrapani and Joseph Contorinis were charged with insider dealing offences. By virtue of the insider trading, illicit profits of approximately US\$7mio were made by Jeffries' Paragon Fund. In total seven individuals were found to be engaged in the insider trading ring which generated a combined total of over US\$1.6mio in illegal profits. Nicos Stephanou served 19 months in custody after his

arrest but was then freed following his co operation in acting as the star witness in the trial and conviction of Joseph Contorinis who received 6 years imprisonment.

Country: US

Key date: 2008 (arrested on insider dealing charges, later convicted and serving 19 months in prison)

Stanko Grmovsek

Canada's first criminal conviction for illegal insider trading occurred in November 2009 when the Ontario Court of Justice accepted a guilty plea from Stan Grmovsek. His co-defendant to related OSC and SEC civil actions, Gil Cornblum committed suicide on 27 October 2009, a day before he was scheduled to plead guilty. Cornblum and Grmovsek collaborated in a deliberate and prolonged illegal insider trading scheme. Cornblum and Grmovsek, who were classmates at law school, started the illegal insider trading scheme after their graduation in 1994. Cornblum sought and obtained inside information about pending corporate transactions that he passed on to Grmovsek who then executed trades in the securities of the corporations involved in the corporate transactions for a profit that they split between them. During the time of the illegal insider trading, Grmovsek worked at a number of law firms in New York and Toronto. Cornblum received some of the inside information in his role as counsel to certain issuers on pending corporate transactions and through conversations with colleagues or other counsel. Cornblum would also use the night secretarial staff's temporary passwords to search for confidential information in the computer databases at the law firms that he worked for. He also conducted early morning searches through the hallways, photocopy rooms, fax machines and files of his colleagues at the firms for documents that contained confidential information about pending transactions that he was not involved in. The illegal insider trading scheme spanned a 14 year period from 1994 to 2008 and in total, Cornblum tipped Grmovsek and Grmovsek traded while in possession of inside information about 46 corporate transactions involving securities that were publicly listed in Canada and the US. In Canada, Grmovsek was charged with three offences: (i) fraud (for trades executed before the new Criminal Code insider trading provisions), (ii) illegal insider trading contrary to the Criminal Code and, (iii) money laundering contrary to the Criminal Code. In January 2010, Grmovsek was sentenced to 39 months imprisonment on the joint recommendation of the prosecution and the defence. In the US, the SEC alleged that Grmovsek violated the anti-fraud provisions, including prohibitions against insider trading. Grmovsek pleaded guilty and was convicted of one count of conspiracy to defraud. He was sentenced to a term of imprisonment of time served. In addition to the jail terms, Grmovsek agreed to disgorge orders to the SEC total of US\$8.5mio with a waiver of all but nearly US\$1.5mio and to the OSC a total of US\$1.03mio.

Country: US, Canada

Key date: 2009 (Canada's first conviction for insider dealing)

Mehmet Sepil

Mehmet Sepil, the chief executive officer of Genel Enerji, a Turkish oil exploration company, was fined £967,005 for dealing in the shares of UK listed Heritage Oil Plc (Heritage) on the basis of inside information. This was the largest fine by the FSA against an individual for market abuse. Genel Enerji's chief commercial officer, Murat Ozgul and Levent Akca, its exploration manager, were also fined £105,240 and £94,062 respectively for dealing in Heritage's shares on the basis of inside information. All three fines include the disgorgement of profits that Sepil, Ozgul and Akca made of £267,005, £35,240 and £10,062 respectively.

On 31 March 2009 Genel Enerji entered into a joint venture with Heritage regarding the exploration of the Miran oil field in Kurdistan. All three executives were actively involved in the joint venture project. As a result of the joint venture, Genel Enerji received detailed daily reports from Heritage of the drilling tests at Miran from 17 April 2009 until 3 May 2009 when the testing concluded. While it was publicly known that Heritage was testing at Miran, the progress and results of the tests were confidential and highly sensitive. On 4 May 2009, Sepil, Ozgul and Akca flew to London together to attend a series of meetings. They also discussed the positive test results. The next day, they all contacted their brokers and purchased shares in Heritage. On 6 May 2009, Heritage announced the results of the Miran testing as a "Major Oil Discovery" with oil-in-place of between 2.3 to 4.2 billion barrels. Following the announcement, Heritage's share price increased by approximately 25%. On the day of the announcement, Sepil, Ozgul and Akca sold all their Heritage shares at a profit. Three months after the trading Sepil, Ozgul and Akca voluntarily contacted the FSA expressing remorse and made certain admissions concerning the basis for their trading.

Country: UK
Key date: 2009 (FSA start proceedings for insider trading after voluntary admissions made)

Special Focus 17 **Raj Rajaratnam**



Raj Rajaratnam, a well connected US based fund manager was convicted in 2011 on 14 counts of securities fraud by earning over US\$60mio trading stocks in companies

including Hilton, Google, Intel and others, based on material, non-public information obtained through an impressive expert network, company employees and other hedge funder managers. The case was described by US Prosecutors as the largest hedge fund insider trading case in US history.

Well before the conviction and based on the allegations against RR, Galleon received requests from investors for the withdrawal of US\$1.3bio, causing the fund to close down. Investors received all of their money back in January 2010, plus profits.

RR started his career as a lending officer at the Chase Manhattan Bank where he made loans to high-tech companies. He joined the investment banking boutique Needham & Co. as an analyst in 1985, where his focus was on the electronics industry. He became the head of research in 1987 and the president in 1991, at the age of 34. At the company's behest, he started a hedge fund — the Needham Emerging Growth Partnership — in March 1992, which he later bought and renamed 'Galleon'. His hedge fund was valued at US\$3.7bio in 2009, down from a peak of US\$7bio in 2008. RR made no secret that his best ideas come from frequent visits with companies and conversations with executives. RR profited from information received from Robert Moffat, an IBM executive, Rajiv Goel, an Intel Capital executive, and Anil Kumar, a McKinsey & Company executive. It was reported that Rajaratnam, Goel and Kumar were all graduates of the Wharton Business School, class of 1983.

Raj Rajaratnam liked to tell people that his first name meant "king" in Hindi, and, coupled with his last name, that made him "king of kings."

Galleon brought RR great wealth. Forbes magazine considered his net worth at US\$1.3bio. He owns homes in the wealthy suburb of Greenwich, Conn., and a condominium at the Setai Hotel in Miami Beach. During the trial, Mr. Rajaratnam's former friends told the jury about lavish vacations including, for his 50th birthday, chartering a private jet to fly dozens of family and friends for a safari in Kenya.

RR maintained that his activity did not amount to insider dealing but was merely a type of research known as mosaic, in which Galleon had a dogged approach to information gathering that once pieced together would form a "mosaic" — a complete picture of a company's prospects that gave it an investment edge over other investors

Mr. Rajaratnam's lawyers argued that all of his supposed

illegal trading was grounded in publicly available newspaper articles, analyst reports and company news releases. For instance, the defence presented evidence showing that before Advanced Micro Devices acquired ATI Technologies, 51 news articles and 6 analyst reports speculated on the likelihood of a merger between the two companies.

Prosecutors accepted that Galleon performed legitimate research, however, they argued, the firm and RR at its head routinely violated traded on the basis of inside tips, including in the AMD case and this gave Galleon and RR an illegal advantage and was a major factor in the trading decision. In the words of a former Galleon portfolio manager who testified during the trial, the firm did its homework, but also cheated on the test.

RR was eventually caught through the tenacity and professionalism of SEC investigator, Andrew Michaelson, who whilst reviewing voluntary disclosures by Galleon, in connection with an earlier enquiry into RR's brother Rengan Rajaratnam, who noticed certain incriminating e mails and instant messages between Rengan and his brother Raj in 2006, which led investigators to suspect trading on the basis of inside tips, based on the Rajaratnans offering incentives. The idea to wiretap those involved and so to deploy investigatory techniques normally reserved for organised crime investigations was a new development in insider dealing investigations where evidence connecting the trades with intent and those with inside information had previously been difficult to establish by traditional means.

Case Example 1

From 2003 to March 2009, RR repeatedly traded in stocks after receiving material, non-public information relating to numerous corporate events for example, upcoming earnings forecasts, mergers, acquisitions, and other business combinations ("Inside Information"). The Inside Information was given as tips by insiders and others at hedge funds, public companies, and investor relations firms—including Goldman Sachs, Intel, International Business Machines Corporation ("IBM"), McKinsey & Company ("McKinsey"), Moody's Investor Services, Inc., Market Street Partners, Akamai Technologies, Inc. ("Akamai"), and Polycom, Inc. ("Polycom"). The evidence at trial included, among other things, recordings of wiretapped phone calls between RR and others including Anil Kumar, a senior partner and director at McKinsey; Rajiv Goel, an employee of Intel; Adam Smith, a portfolio manager and analyst at Galleon; and Danielle Chiesi, an employee of the hedge fund New Castle Partners, all of whom pleaded guilty to insider trading charges.

In one case RR conspired to get confidential information on the US\$bio purchase by Warren Buffett's Berkshire Hathaway of Goldman preferred stock before the September 2008 announcement of that transaction during the height of the Financial crises. A former member of the board of directors of Goldman Sachs and former McKinsey & Company chief executive, Rajat Gupta told Rajaratnam about Berkshire's investment before it became public. Gupta stood to profit as would-be chairman of Galleon International. In March 2011, Gupta was charged in an administrative proceeding by the SEC.

Case Example 2

Anil Kumar former McKinsey & Co partner admitted that he leaked secrets about the elite consulting firm's clients in exchange for US\$1.75mio in hidden payments from RR, including a secret US\$1mio payment for a tip that earned US\$20mio in 2006.

Kumar said the Galleon hedge fund founder told him: "You work very, very hard. You are underpaid. People are making fortunes ... so just keep track of your knowledge and share it with me." Kumar said he tipped RR on deals involving McKinsey clients including chipmaker Advanced Micro Devices, for example, "I told him there were advanced discussions both with Dell and Hewlett Packard," with RR replying "that was very useful information." AMD ultimately announced a pilot programme with Hewlett Packard in February 2004 worth US\$400mio to the chipmaker.

Kumar also described how RR mixed business with pleasure. While the pair sat on deck chairs at the beach outside RR's Miami condo in 2009, he said that RR took a phone call on the beach with a tip that Cisco would be buying another company, information Kumar also traded on using his laptop.

This was the first insider-trading prosecution to use methods that had been mainly reserved for organised-crime, drug and terrorism cases. Some jurors said the wiretaps of RR were the deciding factor. The secretly recorded phone calls between Raj Rajaratnam and his friends and co-workers formed the heart of the government's insider trading case. The government played more than 40 wiretapped phone conversations between Mr. Rajaratnam and his accomplices during the trial and replayed several tapes during the first two hours of closing. Whilst initial concerns about admissibility proved to be confounded, the judge finding in favor of the prosecution, the wiretap evidence, proved fatal for RR. The calls, combined with the testimony of cooperators showed how Rajaratnam cultivated

friendships with cash, trading advice and family vacations in order to obtain inside tips.

The tactics used by the US government in building the case against RR may have significant implications for how at least the hedge fund industry manages its compliance and business practices and concern since has been raised that subsequently investment ideas and trading decisions should be supported with detailed paper trails, and surveillance of electronic communications, from phone calls to emails to text messages, and contacts with insiders would be avoided or controlled which would likely affect the way investment decisions were carried out by the generally secretive hedge fund industry.

Penalty: 11 years sentence, being the longest ever for insider dealing

Actions: systematic insider trading via insider ring

Country: US

Key date: 2009 (arrested and charged with insider dealing)

Malcolm Calvert

Malcolm Calvert, a former equities marketmaker at stock broker Cazenove, was sentenced to 21 months in prison for insider dealing after making £103,883 profit from trades that took place between June 2003 and October 2004. The prosecution is also notable for the involvement of a key witness, Bertie Hatcher, a friend of Calvert, who agreed to provide evidence in the trial having been involved in the illicit dealings himself.

Margaret Cole, director of enforcement and financial crime at the FSA at the time, said: "This is another milestone in our fight against market abuse. It's a misconception that insider dealing is a victimless crime: it damages the very confidence and trust our markets operate on and it must be stopped. "The guilty verdict is a shot across the bow for any city workers who may be tempted to trade using insider knowledge. Our message is simple: if you take part in such activity, you run a very real risk of the FSA taking criminal action against you." The FSA also fined Hatcher, a retired bookmaker and insurance broker £56,098 for market abuse. The FSA found that between 2003 and 2005 Hatcher had profited from inside information, using it to buy and sell about 420,000 shares in six companies. The fine represents the full disgorgement of his share of the net profit from these trades. As part of a settlement with the FSA, Hatcher agreed to provide ongoing assistance to the investigation. In return, the FSA agreed to sanction Hatcher using its regulatory powers rather than a criminal prosecution; Hatcher's fine was also reduced substantially owing to his cooperation. Ms Cole continued: "Hatcher took part in illicit trades using inside information and profited from them, because of this he has received a significant fine. However we were also mindful of the need to encourage others to come

forward and assist in the investigation and prosecution of insider dealing and market abuse, especially where it is suspected that two or more people have been involved and that is why we made an agreement with him.

"Hatcher provided valuable evidence to the FSA, not just about his own misconduct, but also in relation to Calvert.

Country: UK

Key date: 2010 (found guilty of insider dealing in UK, sentenced to 21 months in prison)

Oswyn Indra de Silva

Mr Oswyn Indra de Silva, 37, a resident of Kuala Lumpur, Malaysia, was sentenced in 2010 by the Supreme Court of New South Wales in Australia to two years and six months imprisonment on a charge for insider trading. Mr de Silva pleaded guilty to 12 separate sets of transactions undertaken while he was employed by Macquarie Bank as a fund manager. Mr de Silva was convicted of insider trading for trading in equities and contracts for difference (CFD) products on the Singapore Securities Exchange (SGX) while in possession of information about Macquarie's trading intentions. Mr de Silva admitted purchasing securities in particular stocks, and establishing positions in particular stocks, through his personal trading account at Phillip Securities Pte Ltd prior to Macquarie trading in the same stocks on SGX. Mr de Silva was then able to dispose of his securities and exit his CFD positions and profit from the effect of Macquarie's trading in the underlying stock. This conduct is often described as 'front-running'. The trades were made by Mr de Silva between December 2006 and April 2007 and resulted in a total gross profit of approximately AUD\$1.41 million.

Country: Australia

Key date: 2010 (found guilty of front running in Australia)

John Hartman

In December 2010 John Hartman was sentenced to four and a half years imprisonment, with a minimum term of three years on 25 insider trading related charges brought by the Australian Securities and Investments Commission. In April, Hartman pleaded guilty to all charges which were committed while he was employed by Orion Asset Management Limited (Orion) as its equities dealer. Hartman was convicted of 19 counts of insider trading for trading in contracts for difference (CFD) products while in possession of information about Orion's trading intentions. Hartman admitted to establishing positions in particular stocks through his CFD account at IG Markets prior to Orion trading in the same stocks on the open market. Hartman was then able to exit his CFD positions and profit from the effect of Orion's trading on the underlying stock price. This conduct is often described as 'front-running'. The trades were made by Hartman between July 2008 and January 2009 and resulted in a total

gross profit of approximately US\$1.59mio. Hartman was also convicted of 6 counts of communicating inside information about Orion's trading intentions to an alleged associate between March 2006 and June 2008. In December 2009, Hartman consented to the forfeiture of approximately US\$1.57mio to the Commonwealth under the Proceeds of Crime Act 2002. This amount was formerly the credit of Hartman's account with IG Markets which they were holding as stakeholder.

Key date: 2010 (sentenced to 4.5 years in prison for insider dealing in Australia)

Winifred Jiau & Others

Winifred Jiau, a former consultant with expert networking firm Primary Global Research LLC, was convicted of conspiracy and securities fraud in Manhattan federal court for passing earnings and other information about Nvidia Corp in 2011 (NVDA) and Marvell Technology Group Ltd (MRVL) to hedge fund managers Noah Freeman, a former SAC Capital Advisors LP portfolio manager, and Samir Barai, founder of New York-based Barai Capital Management LP.³¹ Jiau argued at trial that the data she passed wasn't "material," meaning it wasn't something a reasonable investor would consider important for trading a stock and it wouldn't have a bearing on the stock price, but this wasn't accepted by the Jury. Primary Global, based in Mountain View, California, links investors with industry experts at public companies. "Wini Jiau gave new meaning to the concept of social networking," US Attorney Preet Bharara in Manhattan said in a statement. "She used and exploited friends at public companies for the purpose of obtaining, and then selling, inside information." With Jiau's conviction, "another link in a corrupt network has been broken," Bharara said. Three other former Primary Global employees, Daniel DeVore, Don Ching Trang Chu and Bob Nguyen have pleaded guilty in the case. At trial, it was argued that Barai had at least a dozen other people at publicly traded companies who provided him with inside information. Assistant Manhattan US Attorneys Avi Weitzman and David Leibowitz called three co-operators who pleaded guilty to insider-trading charges to describe the scheme, including Freeman. He testified he and Barai paid Jiau US\$10,000 for her insider's tips about the two, California-based chipmakers. Jiau said in e-mails to fund managers that she needed US\$2,000 per source for tips. Jurors also heard several recordings of Jiau's conversations, some of which used codes. Company insiders were "cooks," money was "sugar" and inside information was "recipes," he said. "Cooks are on strike now," Jiau wrote in a 3 June 2008, e-mail. "So drop some of your extra sugar to me," she wrote. "Cooks don't talk to me without sugar." Ex-SAC portfolio manager Noah Freeman, who pleaded guilty to securities fraud, testified at Jiau's trial that he made millions of dollars on illegal inside information using expert networking firms, which he likened to online

dating service Match.com. He said Jiau passed him "perfect information" about Nvidia and Marvell for at least eight quarters, and that he made US\$5mio to US\$10mio on Nvidia and "broke even" on Marvell.

Key date: 2011 (convicted and sentenced to 4 years in prison for insider dealing in US)

Joseph Skowron

Skowron is an Ivy League-educated doctor who left a Harvard University residency programme to become a stock picker on Wall Street. Skowron worked for several prominent hedge funds, before he became the manager of FrontPoint Partners' healthcare funds. FrontPoint was a spinoff from Morgan Stanley. Skowron violated trading restrictions imposed by FrontPoint, in attempting to avoid a loss from adverse hepatitis drug trials conducted at Human Genome Sciences, Inc., a company Skowron's hedge fund invested in. According to the US Attorney's allegations, FrontPoint avoided US\$30mio in losses by selling their Human Genome holdings prior to Human Genome's public announcement of problems with its Hepatitis C drug treatment on 23 January 2008. FrontPoint Partners has not been accused of any wrongdoing, but agreed to pay to a US\$33mio settlement to the Securities and Exchange Commission (SEC), without any admission of guilt. FrontPoint paid US\$900,000 to a firm named Guidepoint Global to gain access to that company's network of experts and consultants. Guidepoint Global is in the business of matching hedge funds with industry analysts. In this case, Dr Yves Benhamou, a 51 year old Parisian infectious disease expert, a consultant to both a biotech firm and the expert networking firm (Guidepoint Global), was paired with Skowron and FrontPoint. According to prosecutor's allegations, Skowron, in violation of FrontPoint ethics rules, made a side deal with Dr Benhamou beginning in 2007. Dr Benhamou, the network expert, allegedly provided insider trading tips to Skowron about Human Genome Sciences, Inc.

The facts and allegations brought forward by the SEC read like an international spy novel to seal their secret arrangement Skowron met Dr Benhamou at a hotel in Barcelona in April 2007 and gave him an envelope with over US\$7,000 in cash. A few months later, Skowron paid for a lavish stay at a New York hotel for Dr Benhamou and his wife. Finally, after getting tipped off about Human Genome, Skowron and Dr Benhamou met in a Milan hotel bar, where Skowron passed an envelope filled with at least \$10,000 in cash to Dr Benhamou in April 2008. Dr Benhamou has since pled guilty to securities fraud charges, conspiracy charges, and for making false statements to FBI agents. Dr Benhamou is co-operating with federal investigators and prosecutors according to the terms of his plea agreement. It is clear that the SEC and federal investigators are paying more attention to relationships between hedge funds and expert network firms, and their temptation to engage in insider trading.

"Prosecutors say expert network relationships are not inherently wrong but that some consultants have crossed the line by taking fees to leak corporate secrets to hedge fund traders and analysts."

Country: US

Key date: 2011 (insider dealing convictions, sentence of 5 years in prison in US)

US Congress

A May 2011 study by Dr. Alan Ziobrowski et al found that members of the US House of Representatives outperform the overall stock market by about 6% annually. The study measured abnormal returns for stock trades made by House delegates from 1985 to 2001 and concluded, "We find strong evidence that Members of the House have some type of non-public information which they use for personal gain." It was a follow up to Dr. Ziobrowski's 2004 Georgia State University study showing that members of the US Senate outperformed the overall stock market by 12%. The Stop Trading on Congressional Knowledge (STOCK) Act first introduced in 2006 was intended to prohibit members of Congress and federal employees from trading stocks based on non-public information obtained on the job, and it would require greater oversight of the growing "political intelligence" industry. The US Senate and the US Supreme Court are the only two out of 975 federal entities that appear to have no rules and no laws prohibiting them from trading stocks based on non-public information they gain on the job. While the US House of Representatives Ethics Manual states that its members should "never use any information coming to him confidentially in the performance of governmental duties as a means for making private profit," it was until recently still legal to do so. On 13 November 2011, CBS' 60 Minutes reported that several members of Congress allegedly used insider information for personal gain. This provided the necessary impetus for Congress finally to act and the STOCK Act came into force in 2012.

Country: US

Key date: 2011 (Published Research indicates members of the US House of Representatives regularly outperformed the stock market in connection with personal investments)

David Einhorn & Others

David Einhorn, the owner of Hedge Fund, Greenlight Capital, whose short selling famously helped to bring down Lehman Brothers bank, was fined £7.2m for insider dealing by the UK Financial Services Authority in 2012. The FSA also fined Alexander Ten-Holter, a trader and former compliance officer at Greenlight Capital, £130,000 for "failing to question and make reasonable enquiries" before selling Greenlight's shareholding in Punch ahead of its fundraising in June 2009, and banned him from holding a compliance job in the future. The FSA has also fined Caspar Agnew, a

trading desk director at JP Morgan Cazenove, £65,000 for "failing to identify and act on a suspicious order from Greenlight to sell Punch shares that allowed the firm to be used to facilitate insider dealing or market abuse". As a result of his failings, the bank failed to identify the trade as suspicious and report it to the FSA. Tracey McDermott, the FSA's then acting director of enforcement and financial crime, said of the Compliance Officer: "Ten-Holter's approach to compliance oversight was wholly inadequate. Serious compliance failures of this nature can have a dramatic effect on the orderliness and integrity of the markets. Agnew was an experienced trader, so should have been suspicious of this transaction and aware of his responsibilities to report it. "Tackling market abuse and insider dealing is not just an issue for the regulator. Compliance professionals and staff on sales and trading desks play a key role in assisting the FSA in detecting and preventing market abuse. Approved persons should be in no doubt as to their responsibilities in this area and the FSA will not hesitate to take tough action where they fall down on these." The FSA said Ten-Holter received an order to sell Greenlight's entire shareholding in Punch on 9 June 2009, despite being made aware that Greenlight had spoken to Punch management a matter of minutes before its decision to sell. The Greenlight analyst who gave the sell-order told Ten-Holter that Punch management would have told them "secret bad things" had they signed a confidentiality agreement and the analyst thought that Greenlight had potentially a window of a week before the stock "plummets". This should have alerted Ten-Holter to the risk that Greenlight may have been in receipt of inside information, the FSA said. On 15 June 2009, Punch announced a fundraising of £375mio, sending its share price down by 29.9%. Greenlight's trading avoided losses of about £5.8mio for the funds under its management, the FSA said. Turning to Agnew, the FSA said his misconduct related to his dealings with Greenlight between 9 and 12 June 2009 when he was instructed by Ten-Holter to sell 11.4m Punch shares, which constituted over 4% of its issued share capital. This represented about 68% of all trading in Punch shares over that period.

Country: UK

Key date: 2012 (fined for insider dealing in the UK)

SAC Capital

US hedge fund SAC Capital Group agreed in March 2013 to pay US\$602mio and US\$14mio to settle 2 SEC charges that it participated in an insider trading scheme and in November 2013 agreed a further settlement of US\$1.2bio. For more details see Part 2, Section 8 SAC Capital below.

Country: US

Key date: 2013 (settled insider dealing claims by paying US\$614mio)

Kidnappers/Robbers/ Extortioners/Forgers

Elmyr de Hory

Elmyr de Hory, a Hungarian, received his art education at Academys in both Munich and Paris, unsuccessfully attempting to make a living as an artist. His career in forgery began with one painting in the style of Picasso that a friend thought was authentic. As a forger, de Hory was distinct for two reasons. The first was his immense talent. Not only could his forgeries fool experts around the world, but he was able to forge paintings by many different artists in many different styles. He faked paintings by Pablo Picasso, Henri Matisse, Amadeo Modigliani, Pierre-Auguste Renoir, Edgar Degas, Alfred Sisley, Claude Monet, and Henri de Toulouse-Lautrec, among others. Secondly, he never copied existing works by the famous artists, but instead painted originals in the style of the artists, which made identifying forgeries more difficult. De Hory claimed he never signed any of the paintings with the name of another artist, and as such denied being a forger, though it's possible that dealers signed the famous names to de Hory's paintings. While de Hory was never convicted of forgery, he still spent a significant amount of time imprisoned, in a colorful life, in a Transylvanian prison for political dissidence, then in a German concentration camp suspected as both a Jew and a homosexual, in Mexico City, where he was jailed on suspicion of murder, and finally in Spain for homosexuality and consorting with criminals. In 1976, de Hory committed suicide, after being informed that Spain had agreed to hand him over to French authorities so he could stand trial on fraud charges. He overdosed on sleeping pills and died like many great artists, penniless. After his death, his paintings (forgeries and originals) became so popular that forged de Horys appeared on the market.

Country: Hungary and elsewhere

Key date: 1976 (committed suicide after being informed that Spain had agreed to hand him over to French authorities so he could stand trial on fraud/ forgery charges).

Gerd Heidemann

Perhaps the most famous forgery to be uncovered in recent times, at least in the 20th Century, concerned a journalist and an experienced forger who almost got away with their crime. Together they would attempt to pass off forged diaries of Adolf Hitler as genuine diaries. The set of documents, contained 62 notebooks "handwritten" as diaries as well as an unpublished third volume of Mein Kampf. The "documents" portrayed

Hitler indifferent to the Jews and largely unaware of any "final solution" of the Jewish people. The crime started in 1981 when the editor of Germany's Stern magazine agreed to buy 27 volumes of what he was assured was Hitler's personal diary, via a staff journalist, Gerd Heidemann, who was secretive about his source, but who advised that he could secure the rights to the diaries for approx US\$2 million. The source was actually an experienced forger, Konrad Kujau who made a living by faking Nazi memorabilia. The journalist, and the forger initially benefited considerably from suitcases of cash given by the editor in order to obtain the diaries. The German magazine were not the only ones to be taken in by the forgeries, as the British Sunday Times also bought the rights and began serialising the diaries in 1983, along with Paris Match and America's Newsweek. In both cases the publications had been examined by experts in both hand writing and history. Nevertheless many were not convinced and the West German police subjected the diaries to a full-scale forensic analysis. Instead of checking the handwriting, the police studied paper and ink. This revealed that the documents were written on paper containing a whitening agent called blankophor, which came into use after 1954. Threads attached to the seals were made of viscose and polyester, artificial fabrics that were not used in Hitler's time. Chromatography identified four different ink types in the diaries. None of these had apparently been available when Hitler was alive. Further ink analysis - measuring the slow evaporation of chloride from the ink - suggested that the writing was less than a year old! Both journalist and forger were imprisoned and each sentenced to four and a half years in prison.

Country: Germany, UK

Key date: 1983 (so called Hitler diaries shown to be forgeries)

Glico-Morinaga

In the 1980's in Japan, a group known as "The Monster with 21 Faces" captured the Japanese public's imagination and many commentators refer to this incident as a turning point in Japanese society, in which the image of a crime-free and safe Japan was dispelled. The Monster with 21 Faces tried to extort 2 Japanese industrial confectioneries Ezaki Glico and Morinaga, over a period of 17 months which started with the initial kidnapping of the President of Glico. In 1984, two masked men wearing caps and armed with a pistol and rifle broke into the home of Katsuhisa Ezaki, the President of Glico. Prior to entering Ezaki's house, the two men had first forced their way into the neighboring home of Ezaki's mother, bound her and took the key to the President's house. Using the key to enter the main house, they then tied up Ezaki's wife and

daughter. Believing the two men were ordinary robbers, Ezaki's wife attempted to negotiate with them for their freedom in exchange for money, but this didn't work. The two men then cut the telephone lines and stormed the bathroom, where Ezaki and his other two children were hiding. Ezaki panicked and cried for help, but was threatened that he would be killed unless he calmed down. The two men abducted Ezaki and held him captive in a warehouse. The next morning, they called the director of the company in Takatsuki city and issued a ransom demand for 1 billion yen and 100 kilograms in gold bullion. However, three days later, Ezaki managed to escape from the warehouse in Osaka.

The kidnapping itself was a crime that was unknown in post-war Japan and shocked Japanese society. The extortion attempts against Glico did not end with the escape of Ezaki. Soon afterwards, vehicles in the parking lot of the Ezaki Glico headquarters were set on fire. Then followed letters from the group calling itself "The Monster with 21 Faces" claiming that they had laced their candies with a potassium cyanide soda. When Glico pulled its products off the shelves at great expense, the "Monster with 21 Faces" threatened to place the tampered products in stores.

The Monster with 21 Faces regularly taunted the police and issued ultimatums to the Media. Eventually, the "Monster" stopped contacting Glico, issuing a letter saying "We Forgive Glico!". However, the "Monster" then turned its extortion campaign on Morinaga and the food companies Marudai Ham and House Foods Corporation. Probably due to the pressure placed on the Police, constantly taunted by the Monster and due to a lack of success to identify and bring them to justice, the local Police Chief, Superintendent Yamamoto killed himself by self-immolation. Five days after the death of Yamamoto, the "Monster with 21 Faces" sent its last message to the media, including the following statement, "No-career Yamamoto died like a man. So we decided to give our condolence. We decided to forget about torturing food-making companies. If anyone blackmails any of the food-making companies, it's not us but someone copying us. We are bad guys. That means we've got more to do other than bullying companies. It's fun to lead a bad man's life. Monster with 21 Faces." Following this message, the Monster with 21 Faces disappeared.

Whilst the case remains officially unsolved, The Tokyo Metropolitan Police suspected that various Yakuza groups had a hand in the Glico-Morinaga case. The end of the blackmail campaign occurred around the time of the Yama-ichi war, the war between the Yamaguchi-gumi and the Ichiba-kai. In addition, Japanese National

Public Safety Commission investigated extreme left-wing and right-wing groups as possible suspects. In 2000, there were rumors in the Japanese media of North Korean involvement in the Glico-Morinaga case.

Country: Japan

Key date: 1984 (Japanese Company President Kidnapped starting a campaign of extortion against confectionary companies in Japan)

Special Focus 18 Northern Bank / IRA



The robbery, one of the largest ever in the UK was of cash and from The Northern Bank headquarters in Belfast, Northern Ireland, believed by the Police and the British and Irish Governments as being the work of the Irish Republican Army (IRA). The claims of IRA involvement are based on the timing, the complexity and organisational professionalism employed but no IRA involvement has been proved and apart from one conviction for laundering some of the stolen cash none of the robbers have been brought to justice. The IRA and their political wing have denied involvement.

The haul included £10mio of uncirculated Northern Bank sterling banknotes, £5.5mio of used Northern Bank sterling notes, £4.5mio of circulated sterling notes issued by other banks, and small amounts of other currencies, largely Euros and US Dollars

Interviewed after the raid, several experts said that taking the Northern Bank notes was foolish, as apart from some tourist destinations, they were essentially useless outside of Northern Ireland and Scotland, and that anyone attempting to pass them in Northern Ireland would quickly arouse suspicion. Following the raid, Northern Bank announced that it would recall all £300mio worth of its banknotes in denominations of £10 or more, and reissue them in different colours with a new logo and new serial numbers. The first of these new notes entered circulation on 11 March 2005.

The operation itself involved the use of the technique known as "Tiger Kidnapping."

On the night of Sunday 19 December 2004 groups of armed men arrived at the homes of two bank officials of the Northern Bank. The gangs identified themselves as Northern Irish police officers and once inside the homes

held the officials and their families at gunpoint. The following day both officials were instructed to report for work at the bank's head office as normal but with specific instructions to assist the gang in carrying out the raid, not to inform anyone else otherwise harm would come to their families. The Bank Officials remained in the office after work, and later in the evening they gave entry to members of the gang. Who then made their way to the bank's cash handling and storage facility. This held an unusually large amount of cash in preparation for distribution to automated teller machines for the busy Christmas shopping season. Cash was transferred to vehicles parked outside in the Street. The gang then fled and later that evening the families were released unharmed.

Whilst some of the monies stolen have since been recovered the bulk of the money remains missing, for example assumed to be a decoy, £50,000 unused Northern Bank notes were found in five packages at a Police Social Club. Only one conviction has been secured in the case though a number of prosecutions were brought. Ted Cunningham an independent Irish Financial Adviser operating via Chesterton Finance a money lending and investment firm and his son Timothy was found guilty in a County Cork courthouse of attempted money laundering. Irish police searching the basement at the Cunningham family home in 2005 found six holdalls and one plastic bag stuffed with cash, £2.3mio to be exact and identified as being from the Northern Bank raid. The authorities believed that Cunningham was given £5mio in 2004 and whilst he looked like a respectable financier, he led a double life as a money launderer for the IRA.

Penalty: found guilty of money laundering
Actions: bank robbery using tiger kidnap technique
Country: Northern Ireland
Key date: 2004 (date of robbery)

Special Focus 19

Ingrid Betancourt



Ingrid Betancourt a Colombian politician, former senator and anti-corruption activist, and Presidential candidate was kidnapped by the Revolutionary Armed Forces of Colombia (FARC) on 23 February 2002 and was rescued by Colombian security forces six and a half years later

on 2 July 2008. The rescue operation, dubbed Operation Jaque, rescued Betancourt along with 14 other hostages (three Americans and eleven Colombian

policemen and soldiers). In all, she was held captive for 2,321 days after being taken while campaigning for the Colombian presidency as a Green. She had decided to campaign in the former demilitarised zone, after the military operation "Tatatos" was launched, and after the zone was declared free of guerrillas by the government. Her kidnapping received worldwide coverage, particularly in France, because of her dual French-Colombian citizenship.

She has received multiple international awards, such as the Légion d'honneur. She was also nominated to the Nobel Peace Prize in 2008.

Most candidates for political office in Colombia in and around 2002 and particularly Presidential hopefuls visited the former DMZ. When Betancourt announced her trip, the government initially confirmed that a security escort would accompany her and she would be transported in a military helicopter, however this offer was soon retracted, and at the same time her body guards received the order to cancel their mission. Not dissuaded, she headed into the DMZ via ground transport, together with Clara Rojas, her campaign manager who was later named running-mate for the 2002 election, and a handful of political aides. According to her kidnapper, the later captured Nolberto Uni Vega, Betancourt ended up at a FARC checkpoint where she was kidnapped. Her kidnap was never planned beforehand, said the rebel. Ingrid still appeared on the ballot for the presidential elections; her husband promised to continue her campaign. She achieved less than 1% of the votes. Alfonso Uribe became President.

A day after Betancourt's kidnapping several non-governmental organisations were organised in the EU and around the world to establish an association or committee for the liberation of Ingrid Betancourt. The committee initially consisted of some 280 activists in 39 countries.

In July 2003 an operation to try to liberate Betancourt was launched but it failed. Whilst negotiated attempts to free Betancourt were regularly explored including exchange of prisoner offers no final agreement could be reached, with failure to reach a deal being blamed by one party each against the other.

In May 2007, a captured Colombian National Police officer John Frank Pinchao managed to escape from FARC captivity, claiming that Betancourt was being held in the same prison camp he had been in. On 18 May, President Alvaro Uribe reiterated his orders for the rescue by military means of Ingrid and other political figures.

Shortly after taking office in mid-May, French President Nicolas Sarkozy asked Uribe to release FARC's "chancellor" Rodrigo Granda in exchange for Betancourt.

On 4 June 2007 incarcerated members from the FARC

were liberated as a goodwill gesture by the government to pursue the liberation of Betancourt and others. However this did not result in her freedom.

With increasing concerns reported over her deteriorating health it was announced on 2 July 2008, that Betancourt and 14 others had been freed by Colombian national forces.

The operation that won their release, codenamed "Jaque" (Spanish for "check" as in checkmate), involved members of the Colombian military intelligence who infiltrated local FARC squads and the secretariat of FARC. The FARC members in charge of the hostages were persuaded to accept a request from headquarters to gather the hostages together, supposedly to be flown to FARC chief Alfonso Cano. Instead, they were flown by government personnel dressed as FARC members to a safe government location.

President Uribe stated that the rescue operation "was guided in every way by the light of the Holy Spirit, the protection of our Lord and the Virgin Mary." The hostages indicated that they had spent much time in captivity praying the rosary, and Betancourt, formerly a lapsed Catholic who prayed daily on a wooden rosary which she made while a hostage, stated "I am convinced this is a miracle."³²

On 21 July 2008, Betancourt and her family made a pilgrimage to Lourdes to give thanks and to pray for her captors and those who remained hostage.

In August 2008, Betancourt and her family were received by Pope Benedict XVI in a brief audience. The liberated Betancourt thanked the Colombian armed forces and President Álvaro Uribe and gave her approval to Uribe's third term as President. She urged neighbouring Presidents Hugo Chávez (Venezuela) and Correa (Ecuador) to help Colombia and seek the political transformations in her country by democratic means. And she stated that she will dedicate herself now to help those who are still held captive in the jungle. Some believe that the liberation of Betancourt caused a dramatic change of the political scene.

In an interview on French radio shortly after her return to France, Betancourt distanced herself from Uribe's approach, while accepting that his security policy had been successful. She said the situation was at a point where "the vocabulary has to change" arguing that "the way in which we talk about the other side is very important". She has also thanked President Hugo Chávez "for his help in recovering the freedom of many Colombian hostages" during a meeting in Caracas in 2010.³³

Sarkozy sent a French Air Force jet with Betancourt's children, her sister Astrid and her family, and accompanied by Foreign Minister Bernard Kouchner for a tearful reunion. After paying her respects at her father's

tomb she and the family boarded the jet and flew to France where she was greeted by Sarkozy and the First Lady Carla Bruni-Sarkozy. She gave speeches and urged the world not to forget and continue for the liberation of the rest of the hostages. She also spent several days in hospital.

On 9 July President Michelle Bachelet of Chile said she would nominate Betancourt for a Nobel Prize. Sarkozy announced that she would receive the Legion of Honor at the Bastille Day celebrations.

On 4 July 2008, Radio Suisse Romande reported that unnamed "reliable sources" had told it the rescue took place after a payment of US\$20mio was made. According to Le Monde, the French Foreign Ministry denied the payment of any ransom by France. Frederick Blassel, the author of the Radio Suisse Romande story, told Colombia's W Radio that, according to his source, the release wasn't negotiated directly with FARC but with César, one of the two guerrillas captured during the operation, who would have received the payment of US\$20mio.

The Colombian Minister of Defence Juan Manuel Santos, and Vice President Francisco Santos, in response to these claims, denied any payment. "That information is absolutely false. It has no basis. We don't know where it comes from and why its being said". He also added with a touch of irony that "Actually, it would have been a cheap offer, because we were willing to give up to US\$100mio. We would be the first to inform publicly, because it is part of our rewards system policy, and besides, it would speak much worse about the FARC." According to Colombia's El Tiempo and W Radio, General Freddy Padilla de León, Commander of the Colombian Armed Forces, denied the existence of any payment by the Colombian government. General Padilla argued that if any payment had been made, it would have been better to make it publicly known, to use it as an incentive and to cause confusion within FARC's ranks. Recent documents made public through WikiLeaks tend to demonstrate that FARC commander Cesar, captured during Operation Jaque and extradited to the US, had offered—prior to the rescue operation—to release Betancourt in exchange for money and protection.

Penalty: released and freed
Actions: kidnapped in 2002 by FARC
Country: Colombia
Key date: 2008 (released by Colombian National forces)

The History Men

A UK based gang dubbed the "History Men" were responsible for creating and selling fake identities to illegal immigrants in the UK. The criminal gang dealt in fake passports with the necessary visas, false National Insurance cards and even forged safety certificates for skilled jobs on building sites.

Realistic-looking utility bills were also part of the detailed "history" produced by the forgers to enable illegal immigrants to find work in the UK and to avoid deportation. The gang charged approx £1,250 for a "history" including a fake foreign passport, National Insurance card, and utility bills that could be shown as proof of address. The histories worked in country, though would not work for airline travel.

Knowledge of the details of the immigration system were important for success for the gang. For example, for a fake Indian passports, residence permits would be included, stamped by immigration officials. Also fake passports may include border stamps from for example, Amritsar in India and Heathrow Airport in the UK as if the holder had returned to his homeland previously to add to the authenticity.

Perhaps more worryingly, the offering can also include certificates such as a fake Construction Plant Competence Scheme card, which list the holder as a "trained operator" for 360-degree excavators. The real nine-day course to learn how to safely operate an excavator and take the necessary theory and practical exams can cost more than £1,500, which can be avoided with a fake certificate. The imposter though could pose a serious threat to workers on sites with potentially dangerous equipment such as diggers.

Following an investigation and prosecution the leader of the History Men gang, Bhavin Shah was jailed for four years nine months in 2012.

Country: UK, India and Indian Sub-Continent
Key date: 2012 (Gang members prosecuted and found guilty and leader sentenced to more than 4 years in prison)

Kiyoshi Takayama

The second most powerful gangster in Japan, and for several years the de facto head of the Yamaguchi-gumi, Japan's largest mafia group (39,000 members), was sentenced in 2013 to six years in prison for extortion by a Kyoto District Court. Kiyoshi Takayama was in de facto control of the Yamaguchi-gumi after its boss Kenichi Shinoda (also known as Shinobu Tsukasa) was imprisoned in 2005, on violations of gun control laws. Shinoda was released in 2011. Kiyoshi Takayama, 65, chairman of the Yamaguchi-gumi Kodo-kai faction, was convicted of extorting cash totaling more than JPY40,000,000 (approximately US\$422,000) from a 67-year-old President of a construction industry in Kyoto under the pretext of "protection money." According to court documents, Kiyoshi Takayama teamed up with Yoshiyuki Takayama (no relation), head of the Yamaguchi-gumi Omi group based in Otsu, Shiga Prefecture, to blackmail the Kyoto businessman on three separate occasions between 2005 and 2006.

The court concluded that Takayama demanded the

businessman work together with the Yakuza, stating at a meeting, "I want you to be on good terms (with Yoshiyuki Takayama) and work together." "Good terms" in the Yakuza world usually means paying protection money or giving in to Yakuza demands. Such extortion is commonplace in Japan where companies are subjected to demands from organised crime syndicates such as for extortion of money.

According to a survey in 2012 by the National Police Agency, 18.4% of company's acquiesced. The figure was almost the same level as a similar survey conducted in 2010 in which 21.8% of companies that received unreasonable demands complied with them. The NPA calls on companies to consult with police when they are troubled by gangsters. The NPA, the Japan Federation of Bar Associations and other organisations conducted a recent survey, targeting 10,000 companies nationwide. The survey asked whether they had received unreasonable demands from organised crime syndicates in the past five years. Among 2,885 companies that responded to the survey, 337, or 11.7%, said they had received such demands from organised crime syndicates. Of the 337 companies, 185 had received such demands within the past year. About 71.8% of the demands pressed companies to pay money, give product discounts or buy items to settle quarrels for which pretexts had been fabricated. Sixty-two of the 337 companies accepted either part or all of the demands. Five companies paid more than 5 million yen, the survey said.

Country: Japan

Key date: 2013 (Yakuza top boss jailed for 6 years for extortion)

Market Abusers

The Tulip Bubble -1634

At the end of the 16th century, the tulip was first introduced from Turkey and soon became a popular flower throughout Europe. In Holland, particularly, the tulip rose to prominence when wealthy Dutchmen coveted them as status symbols. Following a virus the tulip began producing colorful variations in the next generation's petals. Demand increased astronomically and Dutch flower producers and merchants found it difficult to keep up with orders. Dutch merchants tried to control the supply of the new tulips, cornering the tulip market and holding some back, resulting in prices rocketing.

By 1634 speculation in tulip bulbs was rife and a bubble had developed. The most common tulip was the Gouda, which doubled in value to three florins; a craftsman would earn this in about a week. The Centen rose from forty to three hundred and fifty florins; the value of a

small house, and the rare Semper Augustus rose to 6000 florins, the equivalent today of about US\$820,000. With speculators riding the coattails of increasing prices brokers travelled the country from village to village selling a variety of tulip investments to local people, who would often pawn their family heirlooms or mortgage their farms to buy in at current stratospheric prices. By the end of 1636, it seems that the Dutch population had gone tulip crazy, believing that what had previously risen would continue to rise, even though prices bore no relationship to the real worth of a tulip bulb.

With the mania at its height, in 1637 the Dutch government stepped in to dampen the market, believing that the wild speculation was a threat to the economy, which sparked a turn in prices. The Dutch merchants decided that it was time they realized some of their profits and began to sell off their stockpiles of tulip bulbs and within two days, the bubble burst and the market in tulip bulbs crashed. Fortunes were lost as panic now replaced speculation and the country entered into an economic depression

Country: Netherlands

Key date: 1637 (Tulip Mania ended by government intervention, popping the bubble and prices for tulips sent crashing)

South Sea Company - 1720

The South Sea Company was a British company that traded in South America during the 18th century. Founded in 1711, the company was granted a monopoly to trade in South America as part of a treaty during the War of Spanish Succession. However, the areas in question were Spanish colonies, and Great Britain was still at war with Spain. Even once a peace treaty had been signed (The Treaty of Utrecht of 1713), the South Sea Company was allowed to send only one ship per year to Spain's American colonies, carrying a cargo of not more than 500 tons. Additionally, it had the right to transport slaves, although steep import duties made the slave trade entirely unprofitable.

The company did not undertake a trading voyage to South America until 1717 and made little actual profit. Furthermore, when ties between Spain and Britain deteriorated in 1718 the short-term prospects of the company were very poor. Nonetheless, the company continued to argue that its longer-term future would be extremely profitable.

In 1719 the company then began talking up its own stock with "the most extravagant rumours" of the value of its potential trade in the New World which was

followed by a wave of "speculating frenzy". The share price rose from an already lofty £128 in January 1720, to £175 in February, £330 in March and to £550 at the end of May. Shares in the company were "sold" to politicians and senior public figures including the King's mistress at the current market price, however, rather than paying for the shares, these recipients simply held on to what shares they had been offered, with the option of selling them back to the company when and as they chose, receiving as "profit" the increase in market price. This method had the advantage of building support for the Company and in publicizing the names of their elite stockholders, the Company managed to clothe itself in an aura of legitimacy, which attracted and kept others buying and pushing up the stock. Riding the wave of speculation, one Company to go public in 1720 was famously advertised as "a company for carrying out an undertaking of great advantage, but nobody to know what it is" The investment frenzy over the South Sea stock finally led to a price being reached of £1,000 in early August.

The stock would then come crashing down. In August 1720 cash calls were made by the Company on investors who had been allowed to buy shares and pay later. Whilst this scheme had fueled the rise in the shares, the cash call forced many to start to sell the shares to avoid making these payments and to capture profits. As a result of significant sales orders being placed the stock began to fall. Furthermore, "bubbles" were also ending in Amsterdam and Paris which caused a general liquidity crisis and again this pushed South Sea shares down. Once selling gathered sufficient momentum and investors realized the Company's true worth, the price started to fall heavily. By the end of September the stock had fallen to £150 ending up at one hundred pounds per share before the year was out, triggering widespread panic and bankruptcies amongst those who had bought on credit. Company failures now extended to banks and goldsmiths as they could not collect loans made on the stock, and thousands of individuals were ruined, including many members of the aristocracy.

With investors outraged, Parliament was recalled in December and an investigation began. Reporting in 1721, it revealed widespread fraud amongst the company directors and corruption in the Cabinet. Among those implicated were John Aislabie (the Chancellor of the Exchequer), James Craggs the Elder (the Postmaster General), James Craggs the Younger (the Southern Secretary), and even Lord Stanhope and Lord Sunderland (the heads of the Ministry). Craggs the Elder and Craggs the Younger both died in disgrace; the remainder were impeached for their corruption. Aislabie was imprisoned. The newly appointed First Lord of

the Treasury, Robert Walpole was forced to introduce a series of measures to restore public confidence. Under the guidance of Walpole, Parliament attempted to deal with the financial crisis. The estates of the directors of the Company were confiscated and used to relieve the suffering of the victims, and the stock of the South Sea Company was divided between the Bank of England and the East India Company. A resolution was proposed in parliament that bankers be tied up in sacks filled with snakes and tipped into the murky Thames.

Country: UK
Key date: 1720 (South Sea Company share price bubble was popped)

William Duer

William Duer was born in England in 1743, the son of a very successful West Indian planter. Educated at Eton, Duer settled in New York in 1773. Duer was an important man in the city and he also took an interest in politics, supporting the colonists grievances against Britain, and at his wedding in 1779 his bride, the daughter of war general William Alexander, was given away by none other than, George Washington. Duer became a member of the Continental Congress, a New York judge, and a signer of the Articles of Confederation. He was also appointed as an assistant secretary to the Treasury (appointed by the first US Treasury Secretary and good friend, Alexander Hamilton), though he would resign not long thereafter, but not before making extensive contacts and ensuring afterwards that he would continue to be kept informed of banking developments. Duer had made his fortune in land and speculating on the Revolutionary debt. Duer established his own firm with a friend, Daniel Parker. Parker & Duer became a funnel to channel foreign investment to American securities. When Alexander Hamilton sought to strengthen the nations finances through a central bank, Duer was keen to capitalize on the impending opportunity.

Hamilton established the First Bank of the US (BUS) in February of 1791 and the new institution was successful in raising financing mainly from foreign investors, also with Duer's help. Later though Duer in an attempt to corner the market, assembled a group of speculators with the intention of purchasing as many BUS shares and securities as possible. Establishing a group called the "Six Percent Club" with partner Alexander Macomb, the goal was to monopolize the market by buying up to 6% of the government bonds and securities.

In an attempt to manipulate the markets, Duer and his associates started rumors of the creation of a new bank that was to merge with the Bank of the US and

with the Bank of New York. Targeting the taverns and coffee houses, New York soon started to buzz about the potential merger and stock prices rose as a result. The rumors encouraged more speculation and the establishment of two new Banks, successfully driving the New York stock market into a frenzy. But by March of 1792, Duer had not taken his profits and instead rumors began to spread that the bank mergers were not going to happen and the market began to decline. Quickly falling into debt, the decline of the market had a snowball effect, with Duer not only losing his own money, but also the money of those that invested with him. Unable to pay his debts, Duer's creditors had him arrested and placed in debtor's prison.

When news of Duer's financial troubles reached the public, and the fact that many financiers and investors would lose very large amounts the story caught fire, quickly spreading throughout the city. This led to panic and to the stock market crash, which became known as The Panic of 1792. With Duer owing more than US\$750,000 himself, the total losses ran as high as US\$3mio, an enormous sum at the time, representing the savings of nearly every citizen in New York. Many prominent merchants were ruined, adversely affecting trading opportunities and further damaging the New York economy.

On the night of 18 April 1792, a stone-throwing crowd of hundreds descended upon Duer's prison. Threatening the speculator, the prison walls were in fact the only thing keeping Duer safe. With a financial meltdown on his hands, Alexander Hamilton stepped in to resuscitate the damaged economy. Ordering the Treasury to purchase large amounts of government securities, the government intervention helped to stabilize the falling prices. Because Duer often traded on insider information, he earned the distinction of being the first to do so, and has the dishonorable title of being America's first insider trader.

Hamilton, appalled at Duer's speculative activities wrote in 1792. "Tis time, there must be a line of separation between honest men & knaves, between respectable stockholders and dealers in the funds, and mere unprincipled gamblers."

Following the Panic of 1792, those brokers left considered self regulation an imperative. The remaining twenty four brokers created the Buttonwood Agreement, following a meeting under a Buttonwood Tree, in Southern Manhattan in May 1792. The Agreement stipulated in writing that brokers had to be mutually recognised to trade with each other, helping to restrain the infiltration of unethical speculators into the

market. additionally, the agreement would outlaw old trading practices, moving business from environments such as coffee houses to a central location so that dealings could be better controlled and better records kept. The location of that Buttonwood Tree is today 68 Wall Street. In 1817 the Buttonwood Group evolved into a more formal organisation known as the New York Stock and Exchange, which would then become the New York Stock Exchange in 1863. Hamilton tried to intervene on Duer's behalf but was only able to obtain a short reprieve. Duer soon ended up back in prison and he died there in 1799.

Country: US
Key date: 1792 (Duer's activities led to the famous Panic of 1792)

London Stock Exchange Hoaxers of 1814

On 21 February 1814, a man in a British military uniform showed up in an inn on the coast of the English channel and pronounced that Napoleon had been killed and the Napoleonic Wars were now over. Word spread quickly and people began celebrating, this in turn led to the driving up the price of stocks on the London Stock Exchange. Lord Thomas Cochrane was suspected as the culprit, but he was later pardoned by the King after it was determined that he was not involved. The true culprit was never found, though it was still suspected that whoever did start the hoax profited from the increases in stock prices.

Country: UK
Key date: 1814 (rumoring over the false death and defeat of Napoleon allowed some to profit from rising stocks resulting)

NY State Senator Kimble - 1840s

When one of New York's early railroads, the Harlem Railroad, began trading publicly, a state Senator Kimble pushed through a Bill calling for its enlargement. Investors realized that enlargement meant being diluted of their current shareholdings, which led to the process of the stock falling. Kimble and his associates had considered this and had prior to calling for enlargement tried to corner the stock by selling the stock short in significant amounts, making significant profits for himself and his associates at investors expense.

Country: US
Key date: 1840 (market manipulation by attempting to corner the market with others in railroad stock)

Daniel Drew & Others

Jay Gould and Jim Fisk - 1860s onwards - US

The mid 1800s in the US saw the emergence of powerful businessmen and manipulators who would make fortunes for themselves and help transform America into the worlds leading Industrial superpower.

By the turn of the century, these powerful men became referred by Americans as Robber Barons. The term was used to attack these powerful and rich businessmen who had used questionable practices to become wealthy. The term combined the sense of criminal ("robber") with illegitimate social standing ("baron").

The original robber barons were medieval noblemen whose castles overlooked the Rhine. In theory, only the Holy Roman Emperor could set toll rates along Europe's great commercial artery. But the Raubritter, the Robber Barons, exacted unauthorized payments from all passing vessels. In so doing, they added no value to the commerce; no wealth was created by their extortion. Merchants passed the costs on to customers in the form of higher prices. The Raubritter got rich, while everyone else was left a little poorer. US political and economic commentator Matthew Josephson popularized the term during the Great Depression in a 1934 book by the same title. Josephson alleged that American big businessmen amassed huge fortunes immorally, unethically, and unjustly. The theme was popular during the Great Depression amid public scorn for big business. An alternative view however has been advocated by their supporters who acknowledge their ruthlessness and that their standards of behavior would no longer be acceptable in business, but they drove Americas Industrial transformation and they created real and enduring wealth. Moreover, the wealth they created benefited all Americans, they introduced new products, they discovered great efficiencies and they launched businesses that created millions of new jobs. Whatever the view, it is certainly true that the so called Robber Barrons were each very different people with different skills and they were operating at a time when the rules of modern American business were just being written.

They all had, however, some important similarities, with ruthlessness an important trait. Many created fortunes through the emergence of the railroad and its financing, with others involved in the energy that would power Americas Industrial surge. One common theme amongst these powerful men of the Industrial age, was their willingness and abilities as financial manipulators. For example, taking the railroad as an example, some of the Robber Barons fortunes were made by acquiring ownership or control of a railroad and then cashing in by selling railroad securities to a bullish public. In order to acquire ownership and or control the worst kinds of market abuse were practiced. In many cases, they also resorted to bribing government officials to gain favorable contracts or protection from governmental interference. As one would explain in 1877. If you have to pay money [to a politician] to have the right thing done, it is only just and fair to do it.... If a [politician] has the power to do great evil and won't do right unless he is bribed to do it, I think... it is a man's duty to go up and bribe.

Daniel Drew, Jay Gould and Jim Fisk could be considered the original Robber Barons. They manipulated stocks, caused “bear runs” to collapse stock prices and cornered markets. They could get control of companies, pilfer them internally, and then sell out at inflated prices. They spent no time in jail, partly from bribing judges and politicians, but mainly because there were few laws dealing with corporations and markets that could be broken. Gould and Fisk for example attempted to corner the gold market; Treasury Secretary George Boutwell released gold from the federal stock, foiling their plans. After that, Gould bribed judges to void contracts he broke. Jay Gould considered himself to be the most hated man in late-19th century America. He was vilified by the press as a reckless speculator and brutal strike breaker. To many late 19th century Americans, he personified the unscrupulous, greedy Robber Baron. In an age of scandal and corruption, Jay Gould was regarded as a master of bribery and insider stock manipulation. But Gould was much more than a robber baron. At a time when the rules of modern American business were just being written, he was one of the architects of a consolidated national railroad and communication system. One of his major achievements was to lead Western Union to a place of dominance in the telegraph industry. Still he is responsible for trying to corner the gold market, during the presidency of Civil War hero Ulysses S Grant, whose popularity slipped as his Presidency progressed and scandals, particularly the one involving Gould damaged his reputation. On 24 September 1869 the US Gold market collapsed, a day that became known as Black Friday. When the dust had settled at the root of the scandal was Jay Gould. Gould and his associates had tried to corner the Gold Market by buying up as much Gold as they could. Their scheme though was premised on the US government holding on to its Gold reserves because if the government sold it would reduce the effect of their corner and significantly depress prices. Gould had paid off President Grant’s brother-in-law to learn the President’s intentions about government gold sales. Grant, however, learnt of the ruse and eventually ordered the immediate sale of US\$4mio in government gold. Within minutes, the price of gold plummeted, and investors scrambled to sell their holdings in a panic. Many investors had obtained loans to buy gold as the price rose. With no money to repay the loans, they were ruined. Among those who lost big on Black Friday were a number of Goulds’ associates. Gould escaped disaster however by selling his gold before the market began to fall.

Country: US
Key Date: 1860's onwards (the original US robber barons, active in US industry and markets)

Special Focus 20

Stock Market Crash of 1929



For some investors during the 1920s, a financial panic was not a totally new experience. The stock market had shut down for nearly two weeks in 1873, and many could recall when JP Morgan almost single-handedly halted the panic of 1907. Also, the sharp 46% drop between 1919 and 1920 had not been forgotten. But almost everyone agreed that the 1920s were very different. This was the new age of the consumer. Radios, air conditioners, washing machines, and automobiles were all being purchased with “buy-now-and-pay-later” plans. By 1929, consumer credit was helping the average family enjoy the prosperity of the day. Business was good, profits were up, and stocks, which were also being purchased on credit, were soaring. Even though stock prices were reflecting investor optimism, as they normally do, there were also several behind-the-scenes factors that contributed to the high equity valuations and to the vulnerability of the stock market in late 1929. Stocks could be bought on 10% margin in 1929. Any investor could purchase shares having a market value of US\$10,000 with only US\$1,000 of capital. When stocks advanced, the profits generated were being used to purchase additional shares. This leverage, investors soon learned, worked very much in their favour when stocks were rising and, greatly to their detriment, when prices were falling. Perhaps most surprising was the magnitude of the change in stock market credit. In January 1928, total brokers’ loans had reached US\$3.8bio. A year later, the figure had risen to US\$5.3bio, and it continued soaring to a peak of US\$6.8bio in early October 1929.

The late 1920s saw notorious stock price manipulation. Much activity that was considered legal then is no longer permitted today. In 1929, investor “pools” were formed to trade stocks. The pool would buy the shares, use media contacts to spread favourable news or rumours, and then “paint the tape” with large, meaningless trades among themselves. This would draw attention to the stock, allowing the pool to sell the shares, usually at much higher prices, to an unsuspecting public. “Preferred list” sales of new securities at discount prices before the public issues were the norm. Stock pools existed, syndicates established by investment bankers and brokers to manipulate stock price. At this time, prices of at least 100 stocks were openly rigged. Information was considered a private matter, which

allowed companies to manipulate, misrepresent and conceal information.

Michael J Meehan

One of the most infamous manipulations of the time was the RCA pool headed by broker-specialist Michael J Meehan. The pool managed to push up RCA’s stock price by almost 50% between 8 and 17 March 1929. Then, on the very next day, 18 March, the pool sold its entire holdings and divided the profits, about US\$100mio by today’s standards. The first panic occurred on 24 October, Black Thursday. Prices continued down: from a peak of 386 the Dow tumbled to 41 in 1933. The market had no credibility with the public. From 1929 to 1932 11,000 banks failed, gross national product (GNP) declined 10% annually, steel production fell to 12% of capacity, and unemployment hit 25%. In 1929 New York’s two greatest Banks, the Chase and the National City, suffered severely in the aftermath of the Stock Market Crash

Albert H Wiggin

Mr Wiggin was Chairman of Chase National Bank and he was an inveterate speculator and opportunist. In 1929 and in the years preceding the crash he received US\$275,000 in compensation from the Bank. At the same time as leading Chase he was the director of nearly 60 utility, industrial insurance and other company’s, many of whom were clients of Chase and prospective borrowers and from each he received additional compensation. Not satisfied with these extensive interests Mr Wiggin had set up a number of private holding companies in which Wiggin took an interest in stock market transactions, notably profiting famously to the tune of US\$890,000 in transactions in Sinclair Consolidated Oil Company after partnering with a Harry Sinclair who had unique information. However the most noteworthy transaction was probably Mr Wiggin’s transactions in Chase National Bank itself. In one perfectly timed operation he sold short Chase stock and then bought the shares back once the stock price had fallen, benefiting significantly from the crash. Astonishingly these transactions were financed by the Bank itself. The profit was over US\$4mio.

Charles Mitchell

Charles Mitchell was the Chairman at the National City Bank. Prior to the crash Mr Mitchell had been considered a leading prophet of the new era of stock market growth. In 1929 Mitchell was completing the merger of his own Bank with the Corn Exchange Bank but before this could be completed the crash occurred and with it the stock value of his Bank and the currency for the merger went down. In order to save the deal, he borrowed cash from JP Morgan & Co and together with his own money, Mitchell started buying National City stock hoping to support the stock and to see its value rise. With market sentiment still very negative the share support operation failed. Mitchell

would resign later and would be arrested but acquitted on tax evasion charges relating to his shareholdings.

Richard Witney

By the 1930s the political elite and in particular starting in 1932 in the Senate Banking Committee, investigations commenced into questionable stock market practices. Its first witness was Richard Witney, President of the New York Stock Exchange.

Witney’s evidence largely angered the Senators, with Witney accepting no evidence of wrongdoing by stock exchange participants, explaining little about short selling, syndicates and inside information. He also took exception to one Senator’s depiction of the market as a “gambling hell which should be padlocked” and “an invention of the devil”. Further witnesses included Ben “sell em big Ben Smith, Harry Sinclair, Percy Rockefeller and other market operators who had all engaged in large scale market and stock rigging and reprehensible as these activities then seemed only 3 years before they had been regarded with admiration.

It wasn’t until 1938 that Richard Witney would finally be taken down when he was arrested and convicted on charges related to share support activities from 1933-1938 and fraud as he had pledged other people’s stock, custodied with his firm to secure loans used in a share support scheme. Whilst the Senate was very critical of many involved in reprehensible market and share practices, few flagrant breaches of laws or rules were identified.

Those being criticised included America’s leading financier and many of America’s richest and most powerful people. In 1933, US Senate Banking Committee counsel Ferdinand Pecora exposed how JP Morgan & Co used inside information to provide guaranteed profits to former President Calvin Coolidge, Franklin Delano Roosevelt’s sitting treasury secretary, the chairman of the Republican and Democratic national committees, and the CEOs of General Electric, AT&T, and Standard Oil, among others. Pecora’s investigators turned up a ‘preferred list’ of highly placed Americans allowed to buy low and sell high on insider information.

Before the Great Crash of 1929, there was little support for federal regulation of the US securities markets. The scandals that were realised and the longevity and depth of the Depression that followed enabled President Franklin D Roosevelt to make good on his promise of financial reform. Congress, during the peak year of the Depression passed the Securities Act of 1933, following up with the 1933 Banking Act (Glass Steagall Act), followed by the 1934 Securities Exchange Act, which created the SEC, and the Commodity Exchange Act 1936. All these Acts together were designed to restore investor confidence in American capital markets by providing investors and the markets with more reliable information and clear rules of honest dealing.

Country: US
Key date: 1929 (Wall Street Crash)

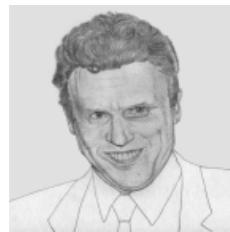
The Hunt Brothers

Nelson and William Hunt were already billionaires and one of the Wealthiest families in America when they tried to corner the global silver market in the late 1970s. As a way to hedge themselves against inflation the Hunts decided to accumulate large amounts of precious metals. Since there were restrictions on private citizens holding gold at that time the Hunt brothers focused on silver. In 1979 working with several Saudi Arabian business partners, the brothers bought up huge quantities of Silver. Before too long, they had amassed over 200 million ounces of silver which was about half of the world's supply. Prices soon started to appreciate. When they started, the price of silver was below US\$5 ounce. By late 1979/early 1980 prices had increased tenfold and were trading near US\$55/oz. During this rise in prices, the COMEX and Chicago Board of Trade (CBOT) only had about 120 million ounces of silver between them. As prices went higher and new buyers got into the market, the exchanges became increasingly fearful of defaulting. As the Hunts owned 77% of the world's silver, either in physical form or futures contracts, the market had been cornered.

Still things were about to change for the worse for the Hunt brothers. Paul Volker was named Chairman of the Federal Reserve. Volker was determined to get inflation under control by raising interest rates. At the same time changes in trading rules at the CBOT and COMEX were introduced, effectively halting silver from going higher. For example, the CBOT set limits on the amount of silver any one entity could hold and raised margins. Not surprisingly prices came down significantly quickly and trading went near to US\$10 by the end-March 1980. It was in late-March 1980 that "Silver Thursday", a day where the price of silver went from roughly US\$20/oz to US\$10/oz, a loss of over 50% occurred. The precipitous drop in prices meant huge losses for many speculators and ultimately forced the Hunt brothers into bankruptcy. By the mid-80s, the Hunt brothers had more than a US\$1bio in liabilities they could not meet. At their peak, the Hunt brothers had held over US\$4.5bio in silver on their US\$1bio investment. On 25 March 1980, the Hunt brothers couldn't meet their US\$135mio margin call, forcing the Hunt brothers to 'shut it down'. The Hunt brothers filed for Chapter 11 bankruptcy in 1988, unable to bear the cost of the legal battles related to their silver scheme. They also paid more than US\$10mio in separate settlements with the Internal Revenue Service and the Commodity Futures Trading Commission (CFTC) and were convicted of conspiring to manipulate the market.

Country: US
Key date: 1980 (Silver Thursday when the price of Silver halved and the cornering scheme fell apart)

Special Focus 21 Michael Milken



Almost no financier in recent times has divided opinion as much as Michael Milken, the "junk bond king" of Drexel Burnham Lambert. His critics cited him as the epitome of Wall Street greed in the 1980s.

Supporters see him as key source behind long term economic gains as he took "the vast sums trapped in old-line businesses and put them back into the markets". Completing an MBA at Wharton, Milken first joined Drexels in 1969 initially on a summer job and then full time as director of low-grade bond research. Whilst at Wharton Milken had been influenced by a research study that showed a diversified portfolio of non-investment grade bonds offered better risk-adjusted returns than a portfolio of high grade bonds. On joining Drexel, Milken was given some capital and allowed to trade. Legend has it he was such a workaholic that he wore a miner's helmet whilst commuting on the bus so he could read company prospectuses in the dark.

In the early 1970s Milken persuaded his boss to let him start a high-yield bond trading department. This was an area that did not receive much attention from the major Wall Street firms, who tended to focus on high grade and frequent borrowers. Milken's team became highly successful and by 1976 his income was estimated at US\$5mio a year.

In 1978 he moved his entire operation one weekend to Los Angeles and eventually opening Drexel's famous Beverly Hills office. There, seated at a vast X-shaped desk with his head trader to his right and his head of sales opposite, Milken built his operation. By the mid 1980s he had established an unparalleled network of high yield bond issuers, buyers and investors. This allowed him to raise large sums at very short notice in the capital markets for lower grade borrowers. CFOs and CEOs from small and medium sized companies beat a path to his door. Many successful entrepreneurs and companies of the 1980s owed their success to Milken's capital raising ability: as he once remarked "there is no shortage of capital; there is only a shortage of management talent". Milken's clients included McCaw Cellular, Time Warner, Viacom, Safeway and

MGM. Milken was also particularly instrumental in the rapid growth of Nevada and Las Vegas helping to finance casinos and house-builders. In short Drexels (through Milken's team) was to all intents and purposes the major underwriter and trader of high yield bonds throughout the 1980s.

More controversially the rapid development of the high yield bond market was the life-blood of the leveraged buyout (LBO) market and so called 'green-mailers'. Those who have watched the film Wall Street will have seen in action at least a form of a fictional LBO. Armed with a "highly confident" letter from Drexels (i.e. Drexels promised to raise the necessary debt to fulfil the buyer's obligations) LBO firms could profit merely by threatening a buy-out of a large blue-chip company in which they had built up an equity position. Milken and Drexel's job was made easier as, at least for a long while, top-tier Wall Street firms were reluctant to compete for fear of jeopardizing their long and rewarding relationships with many of the 'target' blue chip companies.

Although there were suggestions Milken had been under almost continuous scrutiny since the late '70s things got serious when in 1986 the SEC prosecuted Ivan Boesky, a prominent arbitrageur and a possible model for Gordon Gekko in the film Wall Street, for insider trading. In settling his case Boesky implicated Milken in his circle of insider traders. Both the SEC and Rudy Giuliani, the then US Attorney for the Southern District of Manhattan, commenced formal and aggressive investigations of Drexels and Milken.

For 2 years Drexel denied wrong doing claiming the SEC case was based entirely on the statements of an admitted felon (Boesky) looking to reduce his sentence. Nevertheless, in 1988 the SEC sued Drexel for insider trading, stock manipulation and stock parking (buying stocks for the benefit of another). All of the transactions involved Milken and his department.

Around the same time Giuliani began seriously considering indicting Drexel under RICO. This was potentially disastrous as it would require Drexel to put up a performance bond of up to US\$1bio in lieu of having its assets frozen. In early 1989 with literally minutes to go before being indicted (one source indicates the Grand Jury was actually in the process of voting on the indictment) Drexel agreed to plead no contest to 3 counts of stock parking and 3 counts of stock manipulation. It also agreed to pay a fine of US\$650mio and agreed that Milken would leave the firm if he was himself indicted. Drexel was now a convicted felon.

In April 1989 Drexel settled with the SEC agreeing to stricter safeguards on its oversight procedures.

Milken was eventually indicted in March 1989 on an astonishing 98 counts of racketeering and securities fraud under the Racketeering Influenced and Corrupt Organisations Act (RICO) and left Drexel. Perhaps even more astonishing to those on Wall Street was the revelation that Milken's income in 1987 alone was US\$550mio. He eventually settled and pled guilty to 5 relatively minor charges: two related to aiding tax evasion in transactions executed for a client and three related to helping Boesky conceal the real owner of a stock. He was fined and sentenced to 10 years imprisonment, subsequently reduced to 2 years and of which he served 22 months.

Since his release Milken has focused mainly on charitable and philanthropic work and in 2010 still appeared in the top 500 on Forbes list of the world's wealthiest billionaires.

Drexel survived its annus horribilis of 1989. However with business slow and an unexpected crash of the junk bond market, Drexel's found it increasingly difficult to generate profits and finance its operations. Without a large parent Drexel in particular found it nearly impossible to re-borrow under its commercial paper programmes. In early February 1990 it was obvious Drexel was headed for collapse and without a Government bail out on 13 February 1990 Drexel officially filed for Chapter 11 Bankruptcy Protection.

With the benefit of hindsight it seems that the revenue generating capability of Milken and his department became so large within Drexel's overall business that the fate of both became almost inexplicably intertwined. From the earliest negotiations with Giuliani the Government's insistence that any settlement had to include the removal of Milken from the firm was a huge sticking point and an unacceptable step too far for Drexel's management.

Also with the benefit of hindsight one cannot help wondering the extent to which Milken's department based as it was on the West Coast of the US formed, in effect, its own 'firm within a firm' removed from the oversight and governance processes that might apply elsewhere.

Some have noted that Drexel adopted a highly "meritocratic" and aggressive business culture. It is also perhaps noteworthy that Drexel had little ability to bring in outside capital and relied very significantly

on its ability to raise money through wholesale funding including, in particular, its commercial paper programme. It seems that its inability to continue to finance itself through the wholesale markets was the final trigger which led to Drexel's filing for Chapter 11 Bankruptcy Protection.

The zeal and aggression with which the authorities pursued Milken particularly but also Drexel's was astonishing and even at that time caused some disquiet amongst certain commentators and academics. For example, Milken's brother, Lowell was threatened with indictment despite having little obvious connection with the matters under investigation other than increasing the pressure on Milken to settle. Federal investigators also questioned Milken family members including his aging grandfather about their investment activities. The use of the draconian powers available under RICO was largely unprecedented. The wrongdoing to which Milken eventually agreed to plead guilty had never before and has never since been dealt with as a serious criminal matter.

The penalties levied on Milken were ultimately huge and arguably out of all proportion to the crimes for which he was convicted. At trial the judge estimated that the injury for all counts to which Milken plead guilty combined together was US\$318,000. In addition to the 22 months he served in prison Milken accepted a lifetime ban from the securities industry, agreed to pay US\$200mio in fines, and agreed to a settlement with the SEC in which he paid US\$400mio to investors who had been hurt by his actions. In a related civil lawsuit he agreed to pay US\$500mio into a fund to compensate Drexel's investors. In total Milken paid US\$1.1bio for all lawsuits related to his actions while working at Drexel.

Penalty: US\$1.1bio in all fines and penalties and served 22 months in prison

Actions: freewheeling junk bond sales led to downfall of Drexel Burnham Lambert

Country: US

Key date 1989 (Milken indicted on securities fraud charges)

John Kaweske

John J Kaweske ("Kaweske"), a former senior vice president and portfolio manager with the Invesco complex of mutual funds, was fined US\$115,000 in 1995. Kaweske served as portfolio manager for Invesco's Health Sciences Portfolio of Invesco's Financial Strategic Portfolios and the Global Health Sciences Fund. The Commission's complaint alleged that Kaweske defrauded investors by failing to disclose to Invesco

and the funds he managed that he had two conflicts of interest. The first was that he had arranged that commissions would be paid to his son based upon investments being made by Invesco funds under his management. The second was that he was a founder, director, and shareholder of a Canadian company in whose subsidiary he caused Invesco funds to invest. The complaint also alleged that Kaweske failed to report certain personal securities transactions to Invesco and was suspected of front running.

Country: US

Key date: 1995 (Invesco fund manager fined by SEC for conflict of interests and front running)

The Flaming Ferraris

The Flaming Ferraris were a 5 man trading team at Credit Suisse in London who became famous for a short time in 1998. The team led by David Crasanti, a former wrestler from Princeton University in the US, included Harvard-educated Adrian Ezra, who was six times Indian squash champion, and James Archer son of Jeffrey Archer, bestselling author but perhaps more tellingly investigated for insider dealing himself as well as imprisoned for lying in court. James Archer, schooled at Eton, studied chemistry at Oxford was reported to be earning between £100,000 a year plus bonus. The group were named after their favourite rum-and-Grand Marnier cocktail served at the Nam Long Vietnamese restaurant in Knightsbridge, where the traders drank on Fridays after work. They were for a time dubbed by the press, the world's most successful share traders, being lauded for allegedly having made money on all but 12 days in 1998, an extraordinary achievement given the economic turmoil of that year. The five would, it was said, bet up to £3bio a time on a deal, made over US\$100mio for Credit Suisse and now expected to share large US\$mio bonuses.

In fact the five based their reputation on a simple publicity stunt, which involved a public relations consultant and the city editor of the Sunday Telegraph newspaper. The plan was to create a legend around the five, enabling them to claim bigger bonuses and perhaps be head-hunted by a competitor firm. For example, whilst they claimed they were ambushed by the media as they stepped out of their 10-seater stretch limousine outside Nobu, an expensive Japanese restaurant on Park Lane, the reality was that this was an orchestrated publicity stunt. In fact the five were part of a broader group across Credit Suisse including at least 15 other arbitrage traders, taking advantage of anomalies in stock markets worldwide and it is believed that they made far less profit than the £100mio they had claimed. Also the £3bio they bragged of betting on each deal was more

the total gross amount of all the trades carried each year. It wouldn't be long however before the Flaming Ferraris would feel the heat and Credit Suisse and UK regulators would put the brakes on their activities. It started with 24 year old James Archer's (who had only started with CS 4 months earlier) trading heavily in the shares of Enso Stora, one of the world oldest and the biggest paper companies, on 29 December on the Swedish Stock Exchange. Archer had attempted to manipulate the price of Stora, which was in the process of merging with another company. To aid his deception, Mr Archer traded from his mobile phone rather than his recorded phone line at work as he placed orders designed to force the price of the share downwards. If he could force the price down, he knew he could make a profit for his book and help boost his bonus.

The Swedish stock exchange's authorities noticed almost immediately and started an investigation. Credit Suisse fired Archer and his two superiors Ezra and Crasanti for covering up for Archer when questioned about the trading. The UK regulator found Archer guilty but did not feel Ezra or Crasanti were involved in the attempt to manipulate the Swedish market. All three admitted however that they had lied and been deceitful. Each was banned from the Industry. Archer and Ezra had to pay £50,000 while Mr Crisanti had to pay £100,000. Credit Suisse later received a fine from the Swedish authorities for market manipulation violations.

Country: UK

Key date: 1998 (Credit Suisse team of traders disbanded after market manipulation allegations led UK FSA to take action)

California Electricity Crisis

The California electricity crisis also known as the Western US Energy Crisis of 2000 and 2001 was a situation in which California had a shortage of electricity caused by market manipulations and illegal shutdowns of pipelines by Texas energy consortiums, including Enron.

The state suffered from multiple large-scale blackouts, one of the state's largest energy companies collapsed, and the economic fall-out greatly harmed Governor Gray Davis's standing. Drought and delays in approval of new power plants and market manipulation decreased supply, with manipulation responsible for most of the supply squeeze. This caused 800% increases in wholesale prices from April 2000 to December 2000. In addition, rolling blackouts adversely affected many businesses dependent upon a reliable supply of electricity, and inconvenienced a large number of retail consumers. California had an installed generating capacity of 45GW, but at the time of the blackouts demand was 28GW. A demand-supply gap was created by energy

companies, mainly Enron, in order to create an artificial shortage. Energy traders took power plants offline for maintenance in days of peak demand to increase the price. Traders were thus able to sell power at premium prices, sometimes up to a factor of 20 times its normal value. Because the state government had a cap on retail electricity charges, this market manipulation squeezed the industry's revenue margins, causing the bankruptcy of Pacific Gas and Electric Company (PG&E) and near bankruptcy of Southern California Edison in early 2001. The crisis cost US\$40 to US\$45bio.

The California energy market allowed for energy companies to charge higher prices for electricity produced out-of-state. It was therefore advantageous to make it appear that electricity was being generated somewhere other than California. After an extensive investigation The Federal Energy Regulatory Commission (FERC) reporting in 2003³⁴ stated that "...supply-demand imbalance, flawed market design and inconsistent rules made possible significant market manipulation." .. "...many trading strategies employed by Enron and other companies violated the law". Manipulation strategies were known to energy traders under names such as "Fat Boy", "Death Star", "Forney Perpetual Loop", "Ricochet", "Ping Pong", "Black Widow", "Big Foot", "Red Congo", "Cong Catcher" and "Get Shorty". Enron were also accused of "Megawatt Laundering" which is analogous to money laundering, coined to describe the process of obscuring the true origins of specific quantities of electricity being sold on the energy market. Enron CEO Ken Lay mocked the efforts by the California State government to thwart the practices of the energy wholesalers, saying, in 2000, "In the final analysis, it doesn't matter what you crazy people in California do, because I got smart guys who can always figure out how to make money."

S. David Freeman, who was appointed Chair of the California Power Authority in the midst of the crisis, made the following statements about Enron's involvement in testimony submitted before the Subcommittee on Consumer Affairs, Foreign Commerce and Tourism of the Senate Committee on Commerce, Science and Transportation on 15 May 2002: "There is one fundamental lesson we must learn from this experience: electricity is really different from everything else. It cannot be stored, it cannot be seen, and we cannot do without it, which makes opportunities to take advantage of a deregulated market endless. It is a public good that must be protected from private abuse. If Murphy's Law were written for a market approach to electricity, then the law would state 'any system that can be gamed, will be gamed, and at the worst possible time.' And a market approach for electricity is inherently gameable. Never again can we allow private interests to create artificial or even real shortages and to be in control. Enron stood for secrecy and a lack of responsibility. In electric power, we must have openness and companies that are responsible for keeping the lights on. We need to go back to companies

that own power plants with clear responsibilities for selling real power under long-term contracts. There is no place for companies like Enron that own the equivalent of an electronic telephone book and game the system to extract an unnecessary middleman's profits. Companies with power plants can compete for contracts to provide the bulk of our power at reasonable prices that reflect costs.

People say that Governor Davis has been vindicated by the Enron confession." Enron eventually went bankrupt, and signed a US\$1.52bio settlement with a group of California agencies and private utilities on 16 July 2005. However, due to its other bankruptcy obligations, only US\$202mio of this was expected to be paid. Ken Lay was convicted of multiple criminal charges unrelated to the California energy crisis on 25 May 2006, but he died due to a heart attack on 5 July of that year before he could be sentenced. Because Lay died while his case was on federal appeal, his record was expunged and his family was allowed to retain all his property. Enron traded in energy derivatives specifically exempted from regulation by the Commodity Futures Trading Commission. At a Senate hearing in January 2002, Vincent Viola, chairman of the New York Mercantile Exchange, the largest forum for energy contract trading and clearing, urged that Enron-like companies, which don't operate in trading "pits" and don't have the same government regulations, be given the same requirements for "compliance, disclosure, and oversight." He asked the committee to enforce "greater transparency" for the records of companies like Enron.

Country: US

Key date: 2001 (California suffers shortage of electricity due to manipulation of energy markets by market participants including Enron)

Shell

In early 2004, Shell announced that it was writing down 25% of its hydrocarbon reserves, causing a £2.9bio drop in its market capitalisation. Following an investigation by the SEC and the UK FSA they found that Shell had misled investors about the size of its reserves since at least 1998 and that it failed to act quickly enough when evidence that the reserves were materially different from those published came to the attention of senior management. Executives had been aware of the problems at least four years previously. The SEC fined Shell US\$120mio (£66mio) and the UK FSA levied penalties of £17mio for market abuse. The UK fine set a record penalty for Market Abuse.

Country: UK, Netherlands

Key date: 2004 (Shell misled investors about the size of its oil reserves and fined by SEC and UK FSA US\$120mio and £17mio respectively for market abuse)

Ken Mahaffey & Others

Ken Mahaffey, (Merryl & Citi), Tim O'Connell (Merryl), Ralph Casbarro (Citi) & David Ghysels (Lehman) were charged with crimes arising from their participation in a "front-running" securities fraud scheme that generated over US\$600,000 in illegal trading profits between January 2002 and December 2003. Front-running occurs when stock brokers inform traders outside the brokerage firm, such as day traders, that a customer of the brokerage firm has placed a large order to buy or sell a particular stock. This information enables the day traders to trade in the same stock before the customer's order is executed, in anticipation of the movement in price that the customer's order is likely to cause. As a result, the firm's customers may not obtain as favourable a price for the stock as they would have absent the front-running. The stock brokers provided the information in violation of fiduciary and other duties owed to their brokerage firms and customers of the brokerage firms. Between January 2002 and December 2003, the brokers routinely provided day traders at two New York City based day trading firms, A.B. Watley, Inc. ("A B Watley") and Millennium Brokerage, LLC ("Millennium"), with material, non-public customer order information, which was disseminated through internal speaker systems at Merrill, Citigroup and Lehman known as "squawk boxes." The brokers placed telephone calls to the day traders and left the telephones off the hook next to squawk boxes at their respective brokerage firms so that the day traders were able to hear the customer orders that were being broadcast. In exchange for access to the squawk box information, the day traders paid substantial amounts of money to the defendants in the form of commissions from "wash trades" (simultaneously buying and selling the same amount of a security at the same price for the sole purpose of generating commissions) that were generated through brokerage accounts that the day traders opened with the defendants at Merrill, Citigroup and Lehman. Some of the defendants also accepted cash bribes from the day traders in exchange for squawk box access. The indictment alleged that the day traders profited from the scheme by trading in front of the large orders that were broadcast through the squawk boxes. For example, when the squawk boxes disseminated information concerning a large buy order for a particular stock, the day traders would purchase shares of the same stock before the larger order was executed. Alternatively, when the squawk boxes disseminated information concerning a large sell order for a particular stock, the day traders would "short sell" the same securities before the larger order was executed. In either circumstance, the day traders profited from the subsequent movement in price that the large customer order caused. The day traders generated profits of over US\$600,000 by engaging in this illicit trading activity through proprietary accounts at A B Watley and Millennium.

Country: US

Key date: 2005 (guilty pleas entered for front running)

Simon Eagle

Simon Eagle was responsible for a complex and prolonged abusive scheme that deliberately set out to ramp up the share price of Fundamental-E Investments (FEI) for his own benefit. In 2003 Eagle agreed to buy 85% of FEI, an Alternative Investment Market (AIM) listed stock, from its two principal shareholders. He intended to keep 10% of the stock and needed to find buyers for the remaining 75%. Eagle purchased SP Bell Limited, an agency-only stockbroker and became its controller and CEO. He also introduced a number of new clients to the firm, despite knowing that some of the clients had insufficient funds to trade. Eagle's intention was to use SP Bell to sell FEI shares to its clients, generating demand for the stock and pushing its price up. Eagle instructed SP Bell staff to sell FEI shares to clients, many of whom were unaware that the shares were being bought and sold on their behalf.

In order to defer clients having to pay for the shares, many of the trades were rolled over from client to client without being settled. These rollover trades which were carried out by the market maker, Winterflood, breached London Stock Exchange (LSE) rules. The trades carried out by SP Bell and the increases in the bid/offer spread for FEI shares by Winterflood, at the request of Eagle, led to an artificial increase in the share price and gave a misleading impression of demand for the shares. The share price rose from 2.5p in May 2003 to 11.75p in July 2004. The scheme enabled Eagle to secure control of FEI and acquire 10% of its stock. He was also paid a commission of £1.2mio by FEI's original shareholders.

The Financial Services Authority fined Simon Eagle £2.8mio and banned him from working in financial services. The FSA stated that "Eagle deliberately set out to create a scheme to artificially inflate the price of FEI shares. He involved others in his activities and exposed individual clients to serious financial debts of over £9mio.

His conduct breached the LSE's rules, caused significant disruption to share dealing in FEI shares, and damaged confidence in the AIM market. This scheme was rotten throughout and at the core was Simon Eagle. He showed a breathtaking disregard for his clients, for his duty as an approved person and chief executive and for the effect of his scheme on markets. He has played procedural games in an attempt to avoid being held accountable for his actions and this tough action shows that we are determined to keep dishonest cheats, like Simon Eagle, out of financial services."

Trading in FEI shares was suspended in July 2004 leaving over £9mio of unsettled trades which neither SP Bell nor its clients could meet. SP Bell ceased trading and went into administration. The FSA fined Winterflood £4mio in 2008 - one of the biggest fines ever handed out. For details see Part 2, Section 8, below.

Country: UK

Key date: 2008 (UK FSA fined Eagle £2.8 mio and banned from the Industry for market manipulation)

Christopher McQuoid

Christopher McQuoid was the first criminal prosecution for insider dealing brought by the UK authorities in 2008. McQuoid was a solicitor, employed as general counsel at TTP Communications. In May 2006, he was told confidentially that Motorola was planning a takeover bid for TTP. He passed that information to his father-in-law, James Melbourne, and two days before the deal was publicly announced, Melbourne bought shares at 13p each. The takeover price was 45p a share and Melbourne's profit was close to £50,000. Three months later, he gave a cheque for exactly half the gain to McQuoid.

Melbourne's trade was spotted as being suspicious and reported to the FSA. It prosecuted, and McQuoid was sentenced to eight months. Melbourne, aged 75, was given the same sentence, but suspended for 12 months.

Country: UK

Key date: 2008 (first UK criminal conviction for insider dealing)

Dipak Patel & Others

Dipak Patel, a portfolio manager for the US-based Passport Capital, along with Kanaiyalal Baldev Patel, Anandkumar Baldev Patel and Bhoomi Industries, profited by placing and executing orders before the orders of Passport India clients, i.e. front running. The modus operandi was as follows. KB Patel knew when Dipak Patel of Passport India would place his orders and for how much and bought and sold the same shares, timed with Passport's trades. For example, on 26 March 2008, KB Patel placed buy orders at 10.04am for shares of Ansal Properties while Passport India put its buying orders at 11.06am. During the same time, the price moved up from Rs151.95 to Rs155. A minute after Passport bought, KB Patel offloaded his shares, making a profit of Rs1.87 lakh from this move.

The same modus operandi was followed in the synchronised buying and selling of many other shares. During the trading hours, Dipak Patel received or made 40 calls to and from AB Patel and eight calls to and from KB Patel. On 33 instances, the calls with AB Patel were around the time that the synchronised trading was taking place. In five out of eight, the calls were at the time during which buying and selling orders were placed by either KB Patel or Passport India. Amazingly, on many occasions, the front-running and synchronised trades generated tiny profits like Rs6,546. In one case, Gujarat NRE Coke was bought at Rs23 and sold at Rs23.10 for a profit of Rs12,093 while Maharashtra Seamless was sold at Rs270 and bought at Rs268. Nevertheless, SEBI has documented ample evidence to prove that KB Patel was front-running the trades of Passport India.

In another example, on 31 January 2008, KB Patel

bought 63,518 shares of Financial Technologies (FT) and sold the same number of shares when Passport bought 70,897 shares. Dipak Patel and the dealers of Karry Stock Broking Private Ltd were talking about this transaction which SEBI traced to the Bloomberg transcripts. Karry dealers wondered where the supply of FT shares was coming from. Dipak Patel replied: "I know exactly where they are coming from." SEBI's conclusion: "From the above, it can be *prima facie* inferred that Dipak Patel had masterminded both sets of transactions in such a manner that KB Patel benefits from the trades placed before those of Passport India."

The sale proceeds from the transactions between KB Patel and Passport India were deposited in KB Patel's Kotak Mahindra Bank and were subsequently transferred to various other accounts or connected entities of KB Patel. Dipak Patel was found to have remitted funds from his NRE account with Kotak Mahindra Bank to KB Patel's account with Kotak Mahindra Bank in Kadi, Gujarat. The amounts received by KB Patel from Dipak Patel were subsequently transferred to Bhoomi Industries and withdrawn. The mailing address provided to Kotak Mahindra Bank by Dipak Patel in Gujarat is the same as that of KB Patel. Interestingly, KB Patel was authorised by Dipak Patel to operate his account as a mandate holder in the account opening form. Bhoomi Industries is a partnership of KB Patel and AB Patel. Bhoomi has two accounts with Shree Kadi Sahakari Bank Ltd, Gujarat - a current account and a hypothecation account. In the current account of Bhoomi, high cash transactions were seen including withdrawal of Rs41,90,000 on 20 February 2009 and Rs14,00,000 on 25 February 2009. The outflow of funds from Bhoomi Industries provides ample evidence of money laundering in these transactions, according to SEBI.

Country: India
Key date: 2009 (Patel fired for front running in India)

David Mason

David Mason was sentenced in the UK to two years in prison after pleading guilty to 13 counts of unauthorized financial activity, one count of making false or misleading statements or promises, and three counts of money laundering.

Mason operated a Boiler Room, organizing pressurized cold calling focusing on pushing investors to purchase shares in EduVest Plc between November 2008 and May 2009. During that time, he used bogus stockbrokers to defraud 32 people out of £270,000 in the belief EduVest would be listing on the PLUS stock exchange. In fact in 2008, Mason had set up EduVest as an investment vehicle himself, and the vehicle had no business activities.

Boiler Rooms refer to a busy centre of activity, usually selling speculative, questionable, worthless or non-existent securities traditionally by telephone, where a group

of salesmen work using unfair, dishonest high pressure sales tactics, sometimes selling penny stocks, operating schemes such as pump and dump or short and distort or committing outright fraud. The term "Boiler Room" is likely to have originated from the cheap, hastily arranged office space used by such firms, often just a few desks in the basement or utility room of an existing office building or by the high pressure tactics used and equated with high pressure heating appliance or a combination of the two. Whilst many consider boiler rooms a fictional relic of a bygone era, for example many disappeared in the 1990s following the burst of the "dot com bubble," many boiler rooms still operate across the world. Advances in telecommunication technology mean that a company can viably operate from long distances targeting unsuspecting prospective investors. Also the Internet has led to this medium being abused for securities frauds by mimicking traditional telephone scams, and leveraging the internet to provide increased anonymity and increased targeting of investors. Boiler Rooms operate in one country while calling prospective investors in another. The advantage of such an operation is that a company can operate without fear of prosecution from the investor's native legal system.

For example, many boiler rooms contacting prospective investors in the UK will operate from Spanish cities such as Barcelona and Valencia. Mason organised cold calling to sell shares in a company EduVest which he had set up himself and was worthless, taking £270,000 from 32 investors. Another example of Boiler Room activity was Stratton Oakmont a New York, brokerage house founded by [Jordan Belfort](#) that was shut down in the late 1990s, following numerous complaints. His story has recently been turned into a movie starring Leonardo DiCaprio called the "Wolf of Wall Street"

Country: UK

Key date: 2011 (first UK criminal conviction for boiler room fraud)

Christopher Pia

Christopher Pia a former head trader at US hedge fund Moore Capital agreed to pay US\$1mio to settle civil allegations by the US Commodity Futures Trading Commission following allegations that he systematically attempted to manipulate prices of platinum and palladium. Moore paid a US\$25mio fine to settle separate CFTC claims of attempted manipulation and supervisory violations.³⁵ At Moore Capital, Mr Pia revelled in his modest upbringing in the New York borough of Queens, complaining about some hedge-fund managers he considered elitist, according to reports from other traders. Callers to his cell-phone heard the Batman theme song, and he drove an orange Lamborghini. He and Moore founder Louis Bacon would go duck hunting together on a 145-acre island Mr. Bacon bought off Long Island. The CFTC alleged that he tried to artificially move futures prices near the very end of daily trading in a scheme called "banging or marking the close," which involves inundating the market with

trading orders.

Prices in the futures markets for commodities help determine how much consumers pay for everything from a carton of orange juice to a gallon of gas. Closing prices in futures markets are set differently than they are in the stock market, where they are determined by the last trade each day, at 4 pm. In the futures market, the "settlement," or closing price, is the weighted average of all trades during the last few minutes of trading. For palladium, for example, the "closing period" is from 12:58 to 1pm, and for platinum it is 1:03 to 1:05pm. Traders can therefore only seek to manipulate settlement prices around by inundating the market with orders during the last two minutes of trading. Trying to push prices higher in that way is known as "banging the close," and is considered market manipulation under US commodities laws. Manipulation in this way would, if successful, allow traders to potentially profit before prices fall. Mr Pia engaged in banging the close frequently during the seven-month period involved in his case.

The CFTC said Pia, frequently either directly or through a Moore execution clerk, would place buy orders in platinum and palladium at the closing. Such trading can have a big impact in markets such as platinum and palladium, which are thinly traded. In one case for example, Mr Pia told a trader in the platinum and palladium market he wanted to buy futures contracts just before the close. In an instant message, Mr Pia told a clerk his aim was to 'push settlement prices higher.' Mr Pia's orders were executed in the last 10 seconds of trading, constituting a large percentage of trading in the contracts, 'in an attempt to manipulate upward' the prices. Under the CFTC settlement, the 45-year-old Mr Pia, also agreed to a permanent ban in trading CFTC-regulated products in platinum and palladium, such as futures contracts. He also is banned from trading instruments regulated by the CFTC during the closing period, the final few minutes of trading when settlement prices are determined.

Country: US

Key date: 2011 (Pia paid US\$25mio to CFTC to settle civil charges regarding attempted price manipulation of platinum and palladium)

Traffickers Illicit Arms Traffickers

Basil Zaharoff

Known variously as the "super salesman of death", the "mystery man of Europe" the "Monte Cristo of our Time" Zaharoff was the world's first larger than life arms dealer, that many have since attempted to emulate. Basil Zaharoff was the world's first flamboyantly high-living arms dealer, "godfather of the modern BAE", a man who once boasted of starting wars in Africa so he could sell weapons to both sides, who helped arm the great powers culminating in the First World War.

Zaharoff was the model for George Bernard Shaw's Andrew Undershaft, "a profiteer in mutilation and murder" in Major Barbara, and was famed for the size of the bribes he paid to secure business.

Basil Zaharoff was born in Turkey, from an exiled Russian Family in 1849. Apparently his first job was as a guide for tourists and then as an arsonist for the Constantinople firefighters, who reputedly set fires alight so as to extinguish them only after being paid a healthy commission from desperate wealthy families watching their belongings going up in smoke. He then got his first break as an arms salesman, when a friend recommended that Zaharoff succeed him, working for a Swedish arms manufacturer. The then political and military conflicts involving the Balkan states, Turkey and Russia provided an excellent opportunity for the young salesman. Each state was ready to spend to cope with the perceived aggressive intentions of its neighbours.

As a salesman for the Swedish inventor Thorsten Nordenfelt, Zaharoff was known for aggressive and corrupt business tactics. These included selling arms to both sides of conflicts, selling fake or faulty machinery and sabotaging demonstrations. Zaharoff sold munitions to many of the leading nations of the time, including Great Britain, Germany, the Russian Empire, the Ottoman Empire, Greece, Spain, Japan, and the US. Although very little could be proved, Zaharoff was viewed as using large bribes to gain business.

Despite his reputation for corruption, he helped popularise a number of famous weapons and vehicles, such as the Maxim gun (one of the first fully automatic machine guns) and the first true submarine. His relationship with and success enjoyed as a result of his association with the Maxim gun and its inventor, Maxim, led Zaharoff to leave his Swedish employer and take up with Maxim. With Zaharoff's abilities the gun was bought by UK arms manufacturer, Vickers, one of the then giants of the industry.

Zaharoff received cash and shares in Vickers itself and

soon joined the Board of Directors of the Company, that would later become British Aerospace and the BAE of today. Of course the turn of the century and the decade to follow was a time for many European armies to rebuild and modernize. Germany and the UK both saw the need to strengthen and equip their armies with new equipment, including large procurements for the Army and Navy. Vickers and Zaharoff were there, willing and able to accommodate both sides.

After its disastrous defeat by Japan in 1905, Russia too had a need to rebuild its armed forces and looked to Vickers and Zaharoff. With the onset of World War 1, Vickers and Zaharoff, would make their fortunes. Vickers would sell, 4 battleships, 3 cruisers, 53 submarines, 3 auxiliary vessels, 62 light vessels, 2,328 cannon, 8,000,000 tonnes of steel ordnance, 90,000 mines, 22,000 torpedoes, 5,500 airplanes and 100,000 machine guns, supplying both sides. In the post war period, Zaharoff continued selling arms, with conflicts in Greece and Turkey, requiring supplies, but he also remarkably involved himself in two additional ventures, that would prove his eye for an opportunity would not be limited to arms sales.

In 1920 he invested in oil, taking a stake in a new venture that would become British Petroleum, now BP, believing their to be a great future in the oil business and he would invest in the debt-ridden Société des Bains de Mer which ran Monte Carlo's famed but failing casino, making the casino profitable again, and adding to his already considerable fortune.

Country: Turkey, Russia, Europe
Key date: 1914 (greatest achievement and opportunity to sell arms to both sides in WWI)

Adnan Khashoggi

Born in 1935 in Saudi Arabia, Adnan Khashoggi's father was the personal physician to King Abdul Aziz ibn Saud, of Saudi Arabia. Once considered the richest man in the world (worth about US\$40billion in the early 1980s), generated from his activities the world's most successful arms dealer. Khashoggi rubbed shoulders with celebrities, royal families and high society. He was renowned for extravagance, including his yacht, private jets, high priced prostitutes, notorious parties and estates all around the world. Rock band Queen even wrote a song about him, called "Khashoggi's Ship".

In the 1970s he was working with Lockheed, receiving anywhere between 2.5% to 15% commissions on sales of Arms into the Gulf as the Middle East began arming and tensions in the region rose. His other main clients were US Arms companies, Northrop and Raytheon which generated many millions in commissions for himself. Much of the dealings by these Companies became the subject of US Senate Hearings on bribery of foreign officials in the 1970s which would lead to the passing of the Foreign Corrupt Practices Act (FCPA) in 1977.

Khashoggi was also the named arms dealer in the Iran Contra scandal, where the US sold arms to Iran via Israel in violation of an arms embargo to secure hostages, and in addition, finance Nicaraguan Contras.

In 1989, Khashoggi was extradited to the US for allegedly helping the Marcos family steal more than US\$100mio by hiding Mrs Marcos' assets, including ownership of four buildings in Manhattan and a collection of paintings. Khashoggi was acquitted and now lives in Monaco. He is still the subject of a British court order to pay £7mio owed to creditors.

Country: Saudi Arabia, US
Key date: 1989 (extradicted to the US)

Leonid Minin

Leonid Minin was born in Odessa in the Ukraine and in the 1990's and was thought to be one of the Ukrainian Mafia's (Odessa Neftemafija) most important members involved in the lucrative Oil and Gas business around this important Black Sea port. He made his fortune not only in leading one mafia faction profiting from Oil and Gas but also he was allegedly involved in international arms and drug trafficking, money laundering, extortion and other offences. For example, in 1998 through contacts he met with Liberian Dictator Charles Taylor and agreed to supply arms to the Revolutionary United Front militants in Sierra Leone. In one case Minin delivered by Plane, 68 tons of ammunition and weapons which cost about US\$1.5mio, sourced from Russia and the Ukraine. The weapons would be used in the brutal attack known as "Operation No Living Thing" carried out in January 1999, where in less than 2 weeks, at least 6,000 innocent people were murdered and thousands more injured and maimed for life. These shipments would be followed by further bigger shipments over the next 18 months.

In August 2000, while celebrating his recent sales to Liberia, Leonid Minin was arrested by Italian Police. He was found in bed with 4 prostitutes in a hotel in Balsamo, passing around a drug vial, after a tip off, though they did not know he was at this time one of the world's most dangerous arms smugglers. As the room was searched, the Police discovered, US\$500,000 worth of diamonds and US\$35,000 worth in different currencies. The most valuable items however came from Minin's briefcase, as 1,500 pages linked him to the illegal supply of weapons and would lead to his arrest, prosecution and conviction. He was sentenced to two years in prison in Italy. Minin's personal legal problems and his extensive drug use made him an erratic and unreliable partner for the Liberians going forward, but they knew of another who was said to be able to deliver anything to anywhere, having some Planes registered under the Liberian Flag. His name was Viktor Bout.

Country: Ukraine
Key date: 2000 (arrested in Italy and sentenced to 2 years in prison)

Simon Mann

The 2004 Equatorial Guinea coup d'état attempt, also known as the Wonga coup, was a coup attempt against the government of Equatorial Guinea in order to replace President Teodoro Obiang Nguema Mbasogo with exiled opposition politician Severo Moto, carried out by mercenaries and organised by mainly British financiers. Equatorial Guinea has vast oil and gas reserves. Prosecutors alleged Equatorial Guinea's opposition leader, Severo Moto, was to be installed as the new President in return for preferential oil rights to corporations affiliated to those involved with the coup. It received international media attention after the reported involvement of Sir Mark Thatcher in funding the coup.

In March 2004 Zimbabwean police in Harare airport impounded a plane which flew in from South Africa with 67 alleged mercenaries on board. On March 9, 2004 Nick du Toit and 14 other South African and Armenian men were arrested in Equatorial Guinea on suspicion of being the mercenaries' vanguard. The alleged plot leader ex-UK Special Air Service (SAS) officer Simon Mann, was arrested with two colleagues near the runway while waiting for arms to be loaded onto Boeing 727, carrying three crew and 64 former soldiers recruited in South Africa. The majority of those alleged to have been the mercenaries planning to carry out the coup are based in South Africa and ex-members of the 32 Buffalo Battalion, a special force unit that fought for the South African apartheid regime. The marketing manager of Zimbabwe Defence Industries, Hope Mutize, said in court that Simon Mann had paid him a deposit on weapons worth US\$180,000 (£100,000) in February 2004 and indirectly linked Mr Mann to the alleged plot by saying he was accompanied by a South African, Nick du Toit, the leader of the 14 men arrested in Equatorial Guinea. But news of the coup apparently leaked to the South African authorities, who tipped off Zimbabwean intelligence.

Their arms requisition included 20 machine guns, 61 AK-47 assault rifles, 150 hand grenades, 10 rocket-propelled grenade launchers (and 100 RPG shells), and 75,000 rounds of ammunition. Mr Mann, 51, said he wanted the rifles, mortars and ammunition to guard JFPI Corporation-owned diamond mines in volatile parts of the Democratic Republic of Congo. It was alleged that those arrested in Zimbabwe made a stopover in Harare city to buy weapons and expected to join a team in Equatorial Guinea to overthrow President Obiang.

Nick du Toit said at his trial in Equatorial Guinea that he was recruited by Simon Mann and that he was helping with recruitment, acquiring weapons and logistics. He says he was told they were trying to install an exiled opposition politician, Severo Moto, as the new President. In a letter from prison on 31 March Simon Mann told his wife, Amanda, and his legal team: "Our situation is not good and it is very URGENT. They

[the lawyers] get no reply from Smelly and Scratcher [who] asked them to ring back after the Grand Prix race was over!.....We need heavy influence of the sort that ... Smelly, Scratcher ... David Hart and it needs to be used heavily and now. Once we get into a real trial scenario we are fxxxxd." David Hart was ex-prime minister Margaret Thatcher's unofficial adviser during the miners' strike and served as special adviser to Michael Portillo and Malcolm Rifkind in subsequent Conservative administrations. "Scratcher" is thought to be Sir Mark Thatcher and "Smelly" Ely Calil. On 25 August 2004, Mark Thatcher, the son of the former Prime Minister of the UK, was arrested under anti-mercenary laws in South Africa after being accused of helping to finance the coup to remove President Obiang.

Crause Steyl was one of the pilots picked to fly the key planners of the coup in a chartered King 200 twin turbo prop aircraft, registered ZS-NB, who later turned prosecution witness in South Africa. Crause Steyl testified that, "I met Mark (Thatcher) three or four times. He was a partner in the venture. He put in about US\$250,000. The money was wired to my company account in various installments. The helicopters cost about US\$600 an hour plus US\$5,000 each for the pilots and US\$10,000 a month for special insurance." Thatcher has admitted putting money into Steyl's company, Triple A Aviation, but he has said it was to cover the cost of an air ambulance project. Steyl dismissed this explanation. "He knew what was going on," he said. On 13 January 2005, Mark Thatcher, in a South African court, pleaded guilty to helping finance a coup plot in Equatorial Guinea. South African police were able to prove that Mr Thatcher had transferred about US\$285,000 to the mercenaries that were to execute the operation and had met and talked frequently to them prior to the coup attempt. After pleading guilty, he was given a four-year suspended sentence and a fine of about US\$560,000.

Simon Mann paid US\$500,000 towards the plot, according to the South African police. Ely Calil, the Chelsea-based Lebanese oil billionaire who is being sued in London by the Equatorial Guinea regime, is alleged to have raised another US\$750,000 though this is strenuously denied. Mr Calil's solicitor said that he did not wish to respond to the claim that he had raised money for the plotters. But he denied any knowledge of the plot. Karim Fallaha was a Lebanese associate of Mr Calil. He is a director of Asian Trading and Investment in Beirut, which signed a contract with Simon Mann to invest US\$5mio in West African projects. Other than the appearance of his name on a financiers list, there is nothing to suggest he had any involvement in the coup. David Tremain, a South Africa-based British businessman, is alleged to have raised US\$500,000. Mr Tremain is alleged to have been "fronting" for a syndicate of South African and other minor investors. Tremain denies any involvement in the coup.

Jeffrey Archer allegedly made a payment of US\$134,000 (£74,000) into Simon Mann's firm logo logistics account in the days before the failed coup attempt. Lord Archer initially issued a statement through his lawyers stating that he had "no prior knowledge" of the alleged coup and that he had not spoken to Sir Mark for "approximately 10 years". In January, on the same day the plotters were meeting at Sandton, outside Johannesburg, Ely Calil called Lord Archer and the pair apparently spoke for 15 minutes. Other calls followed in the run-up to the coup attempt. A lawyer for the Equatorial Guinea government said in London that telephone records showed four calls between Ely Calil and Lord Archer in the run-up to the coup attempt in March.

Prosecutors said Equatorial Guinea's opposition leader, Severo Moto, based in Spain, offered the group US\$1.8mio and oil rights to overthrow the government. President Obiang accused the US and UK and Spain of backing the plot. The Pentagon denied supporting it, though there appears to be some evidence of some form of prior warning or information being received by American and British Intelligence with little being done to stop the attempted coup. For example it is claimed that Foreign Secretary Jack Straw and minister for Africa Chris Mullin were personally told of the plot on Friday 30 January. After receiving news of the coup, Jack Straw allegedly ordered a change to evacuation plans for British citizens in Equatorial Guinea. Jack Straw had told parliament that the Foreign and Commonwealth Office did investigate if there were any British companies involved in the plot after receiving confidential reports, but failed to find any evidence. British officials, and Jack Straw, were forced to apologise after categorically denying they had prior knowledge of the coup plot.

President Obiang also accused the Spanish government of supporting the plot. The allegation could explain the coincidental position of two Spanish warships off the coast of Equatorial Guinea, at the time of the arrests of the alleged plotters. Miguel Mifuno, special adviser to Equatorial Guinea's President, accused the Spanish government of funding opposition groups in exile and supporting the coup directly.

Country: Equatorial Guinea
Key date: 2004 (failed coup attempt)

Mohamed al-Kassar

Mohamed al-Kassar, alongside his older brother, Ghassan, both of Syrian origin and with close links to the Syrian regime of then President Hafez al-Assad, became notorious arms dealers, starting in the "early 1970s", when the government of Yemen asked him to buy guns and rifles for them. Their modus operandi was to sell drugs, both heroin and hashish and then with the proceeds buy arms to sell on the black market. He settled in Spain after arrests in Copenhagen and

in London, but through his continued arms deals developed a reputation as a wealthy, ostentatious businessman.

The European press soon began to call him "The Prince of Marbella". In 1985 he was the subject of a profile in the French magazine Paris Match, which wrote, "in a few years, this Syrian merchant became one of the most powerful businessmen in the world." The Spanish government alleges that in 1985, al-Kassar sold arms to the hijackers of the Achille Lauro cruise ship, and that afterwards he flew the hijackers' leader, Abu Abbas, to safety in one of his private airplanes. Al-Kassar denied the charge. In fact in 1992, the Spanish government arrested him for his involvement and whilst he spent more than a year in jail once the trial was heard in 1995 he was found not guilty.

In 1987, investigations into the Iran-Contra scandal found that al-Kassar had been paid £1.5mio by someone in the US government to sell arms to Nicaraguan Contras. According to an article in The New Yorker, the money came from "a Swiss bank account controlled by Oliver North and his co-conspirators." In 1992, al-Kassar sold arms to Croatia, Bosnia and Somalia, violating UN arms embargoes affecting all three countries. By July 2006, and after a lifetime involved in shady arms deals, the government of Iraq placed him on their "most wanted" list, calling him "one of the main sources of financial and logistics support" for the Iraqi insurgency. His dealings in Iraq brought him to the attention of the US authorities, who decided to put together a sting to trap al-Kassar, code-named "Operation Legacy". They enlisted a 69-year-old Palestinian former member of the Black September organisation, referred to publicly only as "Samir", who was then being held in a US prison. Samir spent much of 2006 trying to arrange a meeting with al-Kassar, and was finally able to do so in December 2006. By February 2007, Samir had arranged a meeting between al-Kassar and two Guatemalan informants posing as FARC insurgents who claimed they wanted to purchase weapons to use against American military forces. The group met several more times, and at later meetings the informants were wearing hidden video cameras, which recorded al-Kassar agreeing to the terms of the deal. The informants, then convinced him to fly to Madrid to collect his payment, but when he arrived he was arrested and charged with conspiring to kill Americans, supplying terrorists, obtaining anti-aircraft missiles and money laundering. He was then extradited to the US and convicted on five charges, among them money laundering and conspiring to sell arms to suppliers for FARC. He was sentenced to thirty years' imprisonment. His brother was suspected as also involved in the drug and arms trade and died of natural causes in 2009.

Country: Syria, Spain and elsewhere
Key date: 2007 (arrested and extradited to the US)

Tomislav Damnjanovic

Tomislav Damnjanovic is a Serbian businessman and according to the UN not only an arms dealer but an illegal arms smuggler. A former employee of Yugoslavia's national airline, Damnjanovic founded his own company transporting supplies of goods aboard an Ilyushin Il-76 freight carrier, building his air transportation business in the process. Like the more infamous Victor Bout, Damnjanovic has chartered planes throughout Africa, the Middle East and Eastern Europe, supplying everything from humanitarian aid to hand grenades. He has chartered flights and run operations using aircraft based in Sharjah, UAE as did Victor Bout, and but unlike the world's most notorious arms smuggler, he has largely avoided media attention, or arrest.

He is thought to have built his business and honed his skills following the imposition of UN Sanctions placed on Yugoslavia during the Presidency of Slobodan Milosevic during the so called Balkan War's, where he helped secure goods and weapons for the regime, helped ship cash out of the country and helped with the mass cigarette smuggling operation designed to make money for the regime and in so doing helped to defraud the EU of billions in tax revenues and break the Sanctions imposed by the UN. For example, In 1994 Damnjanovic and his Serbian partner Tomislav Miskovic re-located to Cyprus, which was being used by the Milosevic regime to launder millions in hard currency reserves. Flights from Belgrade to Nicosia with bags full of Deutschmarks and US dollars were commonplace. Money was deposited and transferred to a variety of bank accounts in order to purchase arms, oil and other commodities from businesses in Greece, Albania, Panama and Israel. Purchases were made through dozens of shell companies established by regime supporters in Cyprus.

He gained notoriety in 2002 when, while contracted to deliver "millions of rounds of ammunition, guns, grenades and mortars" to aid the US military during the US led Wars In Iraq and in Afghanistan, evidence emerged that he had more than just a chequered past. In fact he had a 15 year history of weapons deals with Libyan, Liberian and the Republic of the Congo officials as well as Al-Qaeda-linked Islamist groups in Somalia in addition to his smuggling for the former Milosevic regime.

In 2007, a UN case study on Damnjanovic referred to him as an "invisible arms trafficker", claiming that he "worked outside the law, transporting weapons for US companies and weapons manufacturers such as General Dynamics and Kellogg, Brown and Root based in America while at the same time using chartered flights

in Africa and the Middle East to illegally supply, among others, Saddam Hussein, Charles Taylor, the Myanmar military junta, Muammar Gaddafi and Islamic militants in Somalia. Not surprisingly Damnjanovic was also linked to other arms dealers such as Victor Bout. Tomislav Damnjanovic is still in business, organizing flights of aircraft to Africa and the Middle East in much the same way he has always done.

Country: Serbia

Key date: 2007 (UN call him an invisible arms trafficker)

Pierre Falcone

The secret arms sale to Angola, dubbed Angolagate during the 1990s, is one of France's worst political scandals. During an arms embargo by the UN on both the Angolan ruling party (MLPA) and the UNITA rebels, the French government facilitated the illegal sale of over US\$790mio in arms to the MLPA including 12 helicopters, 6 warship, 150,000 howitzers, 450 armoured vehicles and 170,000 landmines. Ravaged by decades of conflict and civil war, the illegal arms prolonged the conflict, sustained grand scale corruption, further devastated the economy and infrastructure and led to additional killings of tens of thousands of people. The key facilitator in supplying the arms to the MLPA was French businessman Pierre Falcone, engaged by Angolan President José Eduardo Dos Santos. Falcone and his partner, Russian-born Israeli billionaire Arcadi Gaydamak were part of Santos' inner circle. Falcone especially was hailed a national hero for helping Angola exercise its sovereign right to defend itself against the UNITA rebels. He was given Angolan citizenship and to the dismay of the world, was elected as Angolan's ambassador to UNESCO in 2003.

Falcone sourced the arms from Soviet stockpiles, made funds available for the weapons and arranged bribes to officials and politicians in positions of influence. He reportedly transferred the money via suitcases, offshore bank accounts and intermediaries to Angolan and French officials as well as close associates. He also used different bank accounts using in his company, Brenco Trading Limited to achieve this. It is reported that 70 transfers totalling US\$54mio in illegal bribes were paid to officials and more than US\$21mio was received by Angolan high-level officials, passing through banks in Portugal, Luxemburg, the UK and Switzerland. Falcone reportedly circulated at least US\$60mio through 29 bank accounts with Bank of America. The Angolan money was deposited in the accounts of several French companies in Paris, Geneva and Tel Aviv, and then forwarded to tax havens in the Virgin Islands or Monaco.

In 2007, the French government indicted 42 individuals over the scandal including former politicians and businessmen including the former French Interior Minister, Charles Pasqua, former presidential adviser Jacques Attali and son of former French President Charles Mitterrand, as well as Falcone and Gaydamek for tax evasion, money laundering, selling weapons or taking payment to influence and facilitate the sales.

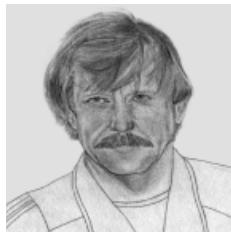
In 2009, 39 of the 42 individuals were convicted of various crimes. However 21 appealed and a number of charges were dropped, including those against Mitterand and Pasqua.

Country: France, Angola, Russia

Key date: 2007 (french indictments for involvement in sanctions busting arms deals)

Special Focus 22

Viktor Bout



Viktor Bout is a former Soviet military translator who made his money through multiple air freight companies which operated in Africa and the Middle East during the 1990s and early 2000s. These companies flew cargo of all kinds including flowers, frozen

chickens, and refrigerators, as well as UN peacekeepers, French soldiers and African heads of state. However Bout is alleged to have presided over the world's biggest private arms dealing network, making hundreds of millions of dollars supplying weapons into conflict zones in Afghanistan, Angola, the Democratic Republic of Congo, Iraq, Rwanda, Sierra Leone and Sudan using his fleet of around 50 aircraft. He was eventually captured in a sting operation organised by the US Drug Enforcement Administration ("DEA") in 2008.

Viktor Anatolyevich Bout was born in Dushanbe, the capital of the then Tajik Soviet Socialist Republic. He joined the Komsomol, the Communist Union of Youth, went on to complete a special training programme with Soviet military intelligence, and then later attended the Military Institute of Foreign Languages in Moscow. Bout is fluent in at least six languages. He has always denied that he was a KGB agent although there is evidence to suggest that he received substantial financial and logistical support from former Russian intelligence

operatives, at least at the beginning of his career.

In the late 1980s, the Soviet army sent Bout to Mozambique and Angola to work as a military translator. At the time Mozambique was a Soviet client state in the cold war against the US. While he was in Mozambique, Bout reportedly met Igor Sechin, who later became Vladimir Putin's chief of staff during his time as deputy mayor of St Petersburg and followed him into the FSB when Putin was appointed its head in 1988. Sechin is currently the President of the Russian oil and gas company Rosneft and appears to have been a powerful source of support for Bout over the years.

Bout was discharged from the military in 1991 with the rank of lieutenant colonel. Shortly after that, the Soviet Union collapsed, providing Bout with an opportunity to start in business. Bout was able to buy up unused planes and unsold weapons at heavily discounted prices. It is alleged for example that, with the help of Russian military intelligence, he acquired three Antonov cargo planes for approximately US\$40k each, a substantial discount to their true value. Using his contacts he was also able to secure access to vast stockpiles of ex-Soviet weapons. Many of the weapons arsenals had been virtually abandoned with the collapse of the Soviet Union and had airstrips inside their compounds making loading easy. With a ready supply of weapons and the means to deliver them, Bout embarked on his arms dealing businesses finding clients in many war torn parts of the world. Bout paid part of the charter money he received from his air freight services to his Russian military intelligence contacts.

Bout had soon managed to acquire a fleet of around 50 aircraft, registering them in jurisdictions such as Equatorial Guinea ("Air Cess") and the Central African Republic ("Central African Airlines") to benefit from their lax regulations. To obtain permission to fly internationally an aircraft must be registered in a country where its maintenance records and air worthiness are certified. By repeatedly registering planes in different countries, Bout was able to avoid local aviation rules, inspection and oversight.

In 1993 Bout moved his fleet to Sharjah in the United Arab Emirates, a hub for flights to and from the former Soviet bloc, the Middle East, Central Asia and Africa. There he met Richard Chichakli, a Syrian born US citizen who became his business partner and long time friend. Chichakli went on to use his expertise as a certified accountant and certified fraud examiner to play a significant part in setting up and managing Bout's companies as well as managing Bout's financial affairs.

Bout does not appear to have had any qualms about dealing directly with warlords and rebels in many of the most dangerous conflict zones. For instance he was happy to deal directly with Jonas Savimbi, the leader of the UNITA rebel group in Angola, supplying him with arms in return for diamonds. Additionally, in the mid 1990s Bout reportedly became instrumental in the supply of weapons to Charles Taylor, a rebel leader who had recently taken power in Liberia and was stoking civil war in neighbouring Sierra Leone. Taylor became notorious for the conscription of child soldiers and the hacking off of limbs. Bout acquired a property in the Liberian capital, Monrovia, from which he attended regular meetings with Taylor at which he negotiated arms sales and was paid in kind with blood diamonds. Bout allegedly employed the services of his own gemstone expert to validate the diamonds as being genuine. Taylor was later extradited in 2006 to the Hague to stand trial on charges of crimes against humanity at the International Criminal Court.

Bout was forced to leave his home in Belgium in 2002 when the authorities there issued an arrest warrant for him. After that he is believed to have travelled to the United Arab Emirates and South Africa and then to Russia. In 2003, Peter Hain, then the British Foreign Minister, coined the nickname "merchant of death", stating that Bout is "the principal conduit for planes and supply routes that take arms....from East Europe, principally Bulgaria, Moldova and Ukraine, to Liberia and Angola".

At around the same time the US government entered into a contract with a company owned by Bout called Irbis Air, an air freight company registered in Kazakhstan. It is not clear whether the US government was aware Bout was the owner of this company. The Irbis Air aircraft were leased to US Air Mobility Command and the defence contractor KBR (which is owned by the Halliburton group) and reportedly completed at least 1,000 flights to Iraq in 2003 and 2004 at a cost to the US tax payer of around US\$60mio.

As Bout's contract became public and the possible implications of continuing to deal with him were explained by the US Treasury Department, the US air force revoked his government contract and placed pressure on private companies using his services to do the same. However, it appears that Bout continued flights for KBR well into late 2005.

In April 2005, new US economic sanctions came into effect against 30 companies which were associated with Bout and these restrictions were adopted by the

UN Security Council eight months later. This should have had the effect of closing Bout's arms trafficking activities but Bout simply incorporated new companies in Moldova and other jurisdictions in Eastern Europe and continued to apply for contracts with the US government, thereby exploiting the tension between the military need to deploy personnel and equipment and the need to conduct due diligence on the firms with whom they were contracting.

The US government placed Bout on a sanctions list in 2006 which had the effect of limiting his freedom of movement. Thereafter Bout stayed in Russia, making only a handful of trips abroad.

Chichakli claimed that he ceased having any business connection with Bout after 2004 but a UN report suggested otherwise and in 2005 he was subject to UN, EU and US sanctions, prompting the US authorities to seize his US\$1.5mio Texas estate and his two Mercedes sports cars. His bank accounts were frozen and his name added to a UN list of arms embargo breakers. Additionally, Bout's brother, Sergei, who is also alleged to have been involved in illegal arms trading was listed as a designated national by OFAC in 2005 and his bank accounts frozen.

One of the interesting features of Bout's activities is that he was prepared to supply arms to both sides in conflict zones. For example, in Afghanistan he initially supplied the Northern Alliance until one of his planes was downed by the Taliban and its crew taken hostage. After negotiations to secure the release of the crew, Bout appears to have started supplying the Taliban with arms using Ariana Airlines (the then official Afghan airline).

The Viktor Bout story also brings into sharp relief the human consequences of the unfettered and unregulated supply of arms around the world. Human Rights Groups and charitable organisations such as Oxfam have campaigned widely for the need to regulate the supply of arms and have complained that UN efforts to establish a global arms trade treaty have been unsuccessful due to opposition from countries which are major arms exporters.

In a sting operation co-ordinated by the Royal Thai Police and the US Drug Enforcement Administration ("DEA"), Bout was arrested in Bangkok on 6 March 2008. Bout had allegedly offered to supply 700 missiles, 5,000 assault rifles, and millions of rounds of ammunition as well as land mines and explosives to people he thought were representatives of the Revolutionary Armed Forces of Colombia ("FARC").

Bout then fought a request from the US government to extradite him and a Thai criminal court ruled in his favour on the 11 August 2009 deciding that the request from the US was politically motivated. This decision was appealed by the US government and on 20 August 2010 a higher Thai court ruled that Bout could in fact be extradited.

Despite protest from the Russian Government Bout was subsequently extradited to the US on 16 November 2010. He was charged by the US Department of Justice with conspiracy to provide material support or resources to a designated foreign terrorist organisation, conspiring to kill Americans, conspiring to acquire and use an anti aircraft missile, illegal purchase of an aircraft, wire fraud and money laundering.

Bout claimed that the US case against him was politically motivated but was convicted by a jury at a court in Manhattan on 2 November 2011 and sentenced to 25 years in prison.³⁶

The chief DEA agent who organised the sting operation told CBS News in a 2010 interview that Bout is "one of the most dangerous men on the face of the earth".

Penalty: 25 years in prison on charges including terrorist charges
Actions: notorious arms dealer known as the "Merchant of Death"
Country: Russia, UAE
Key date: 2008 (Bout arrested in Thailand and extradited to the US)

Drug Traffickers (Organised Crime)

The French Connection

From the 1930s to the early 1970s, the so-called French Connection supplied the majority of US demand for Heroin.

Whilst during the Vietnam War, drug lords such as Ike Atkinson smuggled hundreds of kilos of heroin to the US in coffins of dead American soldiers, it was the so called French Connection which enabled most of the heroin sourced from Indochina, smuggled from Turkey to France and then to Market including the rest of Europe and the US. Whilst the operation started in the 1930s it reached its peak in the late 1960s and early 1970s.

For years, the Corsican Mafia, who controlled the Port of Marseille also controlled the operation. These French traffickers would by 1969 be supplying the Italian American

Mafia in the US with 80 to 90% of its heroin for domestic distribution.

In the early 1970s US law enforcement finally went into action, together with French authorities effectively shutting down the operation and arresting many of its leaders and major participants. The groups involved would either suffer at the hands of the authorities or now weakened would be taken out by now stronger rivals.

The French Connection investigation demonstrated that international trafficking networks were best disabled by the combined efforts of drug enforcement agencies from multiple countries. In this case, agents from the US, Canada, Italy and France had worked together to achieve success.

Country: US, France, SE Asia
Key date: 1970's (US and French Investigators shut down heroin trafficking organisation)

Special Focus 23 Pizza Connection



For those who enjoy a slice of Pizza, Al Dente's Pizzeria located in Queens, New York City is worth a visit. Over 30 years ago, however, this busy Pizzeria was the centre of an international Mafia-controlled drug ring that smuggled 1,650 lbs. of heroin (street value: US\$1.65bio) into the US since 1979 using pizza parlors including Al Dente's as fronts.

Sicilian crime boss and one of the heads of the Mafia worldwide, Badalamenti (the 'boss of bosses' of the Sicilian mafia) purchased opium from Pakistan and Afghanistan, oversaw its production into heroin, then exported it to the US to the New York based Bonanno crime family. Salvatore Catalano a leader of the Bonanno crime family, owned the Al Dente pizzeria and used it as a frequent meeting place for lieutenants in his faction and to make and receive calls concerned with the drug shipments using pizza code where Shipments of heroin were called "cheese" or "tomatoes."

Joseph Pistone, the FBI special agent who famously infiltrated the Bonanno crime family using the alias Donnie Brasco, learned of the operation while undercover and brought it to the attention of the FBI and provided key testimony supplementing evidence obtained by wiretapping over related 300 telephone conversations. Italian Police also discovered cash at the Palermo international airport in Sicily in a suitcase shipped from New York City. The cash was wrapped in pizzeria aprons. These investigations coordinated between New York and Palermo led to the arrest of Badalamenti and Catalano and 30 plus others key organised-crime

figures. Others involved in the case making their names included then US Attorney Rudolph Giuliani says the bust was part of a larger assault on the Mafia. "We can substantially crush organised crime" and led prosecutor, future FBI director Louis Freeh who secured the convictions in a trial lasting from October 1985 to March 1987 of 18 men, including Badalamenti and Catalano. The US government called it the biggest drug and mafia case ever to come to trial in the US. The press called the trial the Pizza Connection.

Starting in the 1960s, the mafia got into the pizza business. In 1968, the Eagle Cheese company opened, which was the first heroin distribution centre. Later, the pizza business provided an ingenious cover for heroin trafficking, and in fact, the mafia came to dominate the pizza business vertically. Many illegal Sicilian aliens worked in these pizza parlors. During this period, huge amounts of narcotics were being laundered through pizza parlor and pizza supply companies. The Sicilian mobsters including Badalamenti dominated the heroin trade, while the American mobsters received a cut for allowing the Sicilians to operate in their territory.

Two nephews of Gaetano Badalamenti operated pizzerias in the US and used them to distribute heroin, not only in Al Dente's Pizzeria in New York City but also out of small mid-western towns, for example, Alfano's Pizza and Spaghetti Restaurant in tiny Oregon, Ill. (pop. 3,800). The friendly Sicilian owner, Pietro ("Pete") Alfano, often tied on an apron and made the pizza himself when he wasn't acting as a "main contact point in the US" for the international drug-trafficking ring.

The Sicilians manufactured and exported cheese, olive oil and tomatoes into the US using also these exports as cover for smuggling drugs alongside. Joe Pistone, aka Donnie Brasco at trial quoted one Bonanno mobster; 'The zips are Sicilians brought into this country to distribute heroin. They set up pizza parlors, where they received and distributed heroin, laundered money. The zips were clannish and secretive...the meanest killers in the business.'

At the end of the Pizza Connection Trial, Gaetano Badalamenti was sentenced to a term of 45 years. He was remanded to the federal penitentiary in Marion, Illinois, a tomblike underground facility known as the worst prison in the US system and died in 2004 aged 80.

"The Pizza Connection trial was indicative of recent prosecutorial approaches to dealing with the Mob. Rather than hunting down an individual capo (boss) or underboss, who would quickly be replaced by the next in line, they would seek to dismantle entire chains of command. This is what they did in the Pizza Connection and would continue to do later for example when they targeted John Joseph Gotti Jr. The "thon don" and Capo of the Gambino crime family, who in 1992 was found guilty and sent also to Marion, Illinois, where he was held in virtual solitary confinement. On 10 June 2002, Gotti died of throat cancer at age 61. In the wake of his conviction, the assistant director of the FBI's New York office, James Fox, was quoted as saying, "The don

is covered in Velcro, and every charge stuck."

These groups don't limit themselves to drug running, though. They're also involved in illegal gambling, political corruption, extortion, kidnapping, fraud, counterfeiting, infiltration of legitimate businesses, murders, bombings, and weapons trafficking.

One area of particular interest for the Italian American Mafia was labour racketeering taking over effective control of some labour unions, providing a rich source for organised criminal groups to exploit. There are approximately 75,000 union locals in the US, and many of them maintain their own benefit funds. Labour racketeers attempt to control health, welfare, and pension plans by offering "sweetheart" contracts, peaceful labour relations, and relaxed work rules to companies, or by rigging union elections. In the mid-1980s, the Teamsters, a 1.4 million-member union, controlled more than 1,000 funds with total assets of more than US\$9bio.

For decades, the Teamsters has been substantially controlled by La Cosa Nostra. In recent years, four of eight Teamster presidents were indicted, yet the union continued to be controlled by organised crime elements, with persistence the government has been fairly successful at removing the extensive criminal influence at the Teamsters.

Penalty: Gaetano Badalamenti, mafia don, sentenced to 45 years imprisonment

Actions: Pizza Houses used as fronts for mafia to launder money

Country: US

Key date: 1985 (trial started to convict Italian Mafia following undercover work of Joe Pistone, aka Donny Brasco)

La Mina/Operation Polar Cap

In 1989, details of Operation Polar Cap was revealed, it being the largest money laundering investigation in the US at that time.

The operation targeted "La Mina", or "the Mine" an enterprise that handled illegal drug profits belonging to the Medellin cartel of Pablo Escobar. La Mina was organised in Los Angeles by a money launderer named Raoul Vivas, acting on behalf of the Colombian drug cartel in Medellin, he would take 5 % commission on all transactions.

Vivas owned a gold refinery in Argentina and another in Los Angeles called Rose Marie Refiners and used his knowledge of the precious metals and jewellery business to launder almost US\$1.2bio in drug proceeds in only 2 years. In one scheme he recruited several existing gold dealers and jewellery companies, who whilst established and legitimate within months, all but abandoned their real businesses and immersed themselves in laundering for Vivas. Two of these Companies, Ropex Corporation and Andonian Brothers Manufacturing Company, were located in the Los Angeles Jewellery Mart. These jewellery businesses each acted to launder enormous sums generated from the sales of drugs,

essential acting as “fronts” for the drug traffickers. Cash deliveries to the “fronts” were boxed and shipped cross-country via armored car with one such shipment of US\$4.8mio being seized as the operation was rolled up. Large shipments of cash had been commonplace over a 2 to 3 year period totaling hundreds of millions of dollars from purported gold and jewellery businesses located in Los Angeles, New York and Houston as payment for fictitious gold and jewellery sales.

In another scheme, Trend Precious Metals and Saccoccia Coin Company, two East Coast precious metals and jewellery Companies, owned by Steven Saccoccia would receive large volumes of cash which would be delivered by courier from New York City, shipped by armored car or private vehicle, to either of these two companies on Rhode Island. Once in Rhode Island, the money would be counted on an automatic counting machine and sorted. Pursuant to Saccoccia’s instructions, it would then be taken to area banks and used to purchase cashier’s or treasurer’s cheques. These transactions were frequently “structured” so that the amounts were less than US\$10,000 – a device designed to avoid the filing of a Currency Transaction Report. On other occasions, when the purchases exceeded that amount, the defendants caused false reports (or no reports at all) to be filed. The cheques were made payable to Trend or other dummy companies controlled by Saccoccia businesses ostensibly engaged in such trades as gold or jewellery that would be expected to generate large quantities of cash. cheques would be deposited in those companies’ accounts, and the funds later transferred to a central account maintained by Trend at a Providence bank. From there, the money would be wired to bank accounts in Colombia and elsewhere, including Europe. In this scheme Vivas imported gold-plated lead bars from Uruguay. The gold plating fooled customs, as the entire bars were described as gold bars, which justified Vivas overpaying massively for the goods, effectively moving drug proceeds from the US offshore. The lead was sold on invoiced as gold still to US based established jewellery companies that were happy to help as part of this laundering operation and from numerous paper shell companies. The 10% that was really gold was sold to responsible precious metals dealers that were none the wiser and saw these transactions as entirely legitimate, providing Vivas though with much needed credibility in the industry. The Cash coming into Vivas was sent by armored car in cardboard boxes. They were labeled scrap jewellery but they were actually stuffed with US\$50,000 to US\$300,000 in dollar bills. Once received they would then deposit the funds in banks, who were told these were the proceeds of legitimate sales of gold and jewellery which could be evidenced by the invoices issued. Once banked, funds would then be wired to the house bank, Banco Occidente, a Colombian Bank, with branches in numerous locations including in Panama.

Another scheme involved Ronel Refining in Florida , which refined precious metal scrap. Vivas contacted Ronal in 1986 with the offer of refining scrap gold material from Uruguay. Ronal was having difficulty making money and so jumped at this new business opportunity.

Ronal should have been suspicious as Uruguay does not have any Gold mines, nor is it noted for its Gold exports. Instead of importing the Gold as proposed, Vivas used the proceeds from drug sales to buy fine gold from dealers in the US. He mixed the Gold with 10% silver and shipped it to Ronal. Vivas could show Ferris that the material was from Uruguay with the import documentation from the gold plated lead bars (see above). As requested Ronal refined the gold and sold it on, paying Vivas, directly into his Banco Occidente accounts, allowing Vivas to effectively launder the drug monies.

Very soon volumes increased, with initial volumes of 10 kilos a day soon thereafter to 80 kilos and then to 300 kilos within two years. As the volumes increased the costs of transportation of the gold from LA to Miami also increased and so in order to reduce costs, Ronal suggested the use of Pooled accounts. The pool account mechanism let Vivas generate all the volume he needed without the cost of moving gold from LA to Miami and back. Vivas opened a metals account with an LA based metals trader. Vivas would pay cash to the Metals trader in LA, and then buy gold from a dealer for Vivas with the cash. Vivas would then release the Gold to Ronal who also held a metals account with the Metals trader. Ronal then sold the Gold to the trader and paid the funds again to started as a depository account at Prosegur’s Los Angeles vault. Vivas would deposit cash into Prosegur. Prosegur would count it, file the Cash Transaction Reports, and remit the funds to a dealer to pay for Vivas’ gold purchases. Vivas would then release the gold to Ronal. Ronal sold the gold to the dealer and remitted the proceeds to Banco Occidente. It was a continual loop where no physical gold even changed hands, the purpose simply being to launder the original drug proceeds and Ronal and the LA metals trader, being the conduits and taking a fee for their support.

Operation Polar Cap led to the first conviction of a foreign financial institution, Banco de Occidente/Panama, for violating US money laundering laws. As a result of this operation, over 100 people were arrested, and more than US\$105mio in assets, including currency, bank accounts, real estate, jewellery, gold, and vehicles were seized. US\$7mio forfeited by the Banco de Occidente/Panama was shared with other governments, including Canada and Switzerland, which each received US\$1mio.

Country: US, Colombia

Key date: 1989 (details of Pablo Escobar’s drug trafficking and money laundering operation revealed)

Special Focus 24

Lucy Edwards and Peter Berlin



It was the early 1990s and BoNY saw an opportunity to expand its business in the emerging Russian market following the collapse of the Soviet Union. In order to do this, it created an Eastern European Division (EED) that was staffed mostly with Russian émigrés, including Lucy Edwards. It was headed by

Natasha Gurfinkel Kagalovsky who was married to Konstantin Kagalovsky; who was a politically connected Russian financier who had been an advisor to Yeltsin and in the early 1990s was Russia’s IMF representative and who then moved to the once-powerful Menatep Bank in Moscow.

BoNY’s quick thinking paid off and they earned a leading position among US banks in handling correspondent accounts for Russian banks. According to US Authorities, “By the late 1990s, the EED was generating more than \$40 million in annual revenues for BoNY and Russia had become the single largest producer of funds transfer revenues among BNy’s foreign operations.” Much of this success was aided by a proprietary electronic banking software product that BoNY acquired from Irving Trust through a hostile takeover during the 1990s and renamed “Micro/CA\$H-Register”; [although similar products were available from all major commercial banks at that time].

BoNY’s software allowed customers (with an apparent business need) to effect wire transfers by themselves (direct access), without the assistance, control or supervision of BoNY employees. Obviously, the software created enhanced risks for money laundering but there were no AML policies or procedures at the time that restricted who could use the product or that required enhanced monitoring on accounts that used the software.

In late 1995, a then 37-year old Edwards was approached by Russian bankers and they worked out an agreement that her husband, fellow Russian émigré, 41-year old Peter Berlin would open up an account at BoNY and obtain the Micro/CA\$H software so that they could make wire transfers to the bank themselves. In 1996, Berlin opened accounts at the One Wall Street retail branch of BoNY in the names of Benex International Co., Inc. (Benex) and BECS International LLC (BECS). The same address was listed on the accounts at BoNY: 118-21 Queens Boulevard, Suite 612, Forest Hills, New York. This was an office that was occupied by an entity named Torfinex Corp. (Torfinex) that was run

by Volkov and became known as the “Queens Office”.

It was a good arrangement as Torfinex was also transmitting questionable money on an unlicensed basis and even applied to the NY State Banking Department for a license in November 1997, a month after they had been ordered by the Department to cease and desist transmitting money. Shortly after establishing the accounts, Berlin obtained the Micro/CA\$H software to facilitate wire transfers and Edwards installed it at the Queens Office. For their efforts, Edwards and Berlin would receive a percentage of the money transferred or commissions, which ultimately totalled US\$1.8mio. Shortly after the operation was set-up, Edwards was transferred to BoNY’s London office in 1996 and they started to pay a BoNY administrative assistant, Kudryavtsev, US\$500 a month to make sure the operation continued to run smoothly.

Benex, BECS and Torfinex were front companies for Depozitarno Klirinogovy Bank (DKB) a Russian bank, whose principal owners were MDM (Moscow World Business Bank) and SobiBank. The accounts were part of an underground unlicensed money transfer business that was operated between DKB from Moscow and the Queens Office. In addition to not being licensed as a money transmitter, the Queens Office was not even licensed as a branch or agency of a foreign bank. These facts would be some of the things that Berlin and Edwards would plead guilty to among others.

For three and a half years starting in February 1996, approximately US\$7bio flowed through the Benex and BECS accounts at BoNY. Hundreds of international wire transfers would be processed daily. More than 150,000 wire transfers were sent during this period and these accounts were the most active at the One Wall Street branch where they brought in wire transfer revenues of approximately US\$1mio. The ordering parties for most of the incoming transfers were from “banks” located in jurisdictions identified by FATF as having a high risk of money laundering activity. The most frequent ordering party was “Sinex Bank Inc.”, which was named as the ordering party on more than US\$3bio of wire transfers during the same 3+ year period. As a result of the investigation, BoNY learned that Sinex Bank was a shell bank registered in Nauru and not surprisingly one of its directors was Volkov. It was controlled by the principals of DKB and created exclusively to assist their illegal money transfer business. The money would then be transferred out of BoNY to multiple third party beneficiaries in offshore banking jurisdictions or to jurisdictions identified by FATF as having a high risk of money laundering activity.

Edwards and Berlin were finally sentenced in July of 2006 to five years’ probation and six months in home detention in New Jersey. They also had to make restitution of US\$685,000 to the Internal Revenue Service and pay fines of US\$20,000 each. Four years earlier, Kudryavtsev was sentenced to two weeks in prison and house arrest for five and a half months. Edwards’ supervisor, Natasha Gurfinkel Kagalovsky, was suspended by BoNY in 1999. She subse-

quently resigned from BoNY and moved to London and was never charged with anything.

Penalty: convicted on money laundering charges
Actions: laundering of US\$bioms in Russian money laundered

Country: US, Russia

Key date: 1999 (Investigations started into massive money laundering from Russia through the BoNY

Speed Joyeros

Speed Joyeros and Argento Vivo were both related Companies in the business of selling gold and silver jewellery and precious metals to many retail and business customers throughout Central and South America as well as also in Europe and the Middle East. They were based in Colon, the Panama free trading zone is the world's second-largest free port, after Hong Kong which, on the edge of the Panama Canal, is home to around 1,600 companies. The 1.5-square-mile zone is home to a multitude of global traders: Arabs, Chinese, Indians, and others and more than US\$6bio of merchandise passes through the Zone each year with as much as a quarter of it, say some in Law Enforcement, financed by drug money. Speed Joyeros was for a time very successful, with revenues of US\$150mio in 1998 and US\$105mio in 1999.

The Companies acted as de facto intermediaries for the Colombian drug cartels, receiving regularly at least US\$10mio via any means, by wire or cheques or even physical cash from the drug traffickers relating to sales of drugs in the US and converting that cash and exchanging it for gold, both in ingot and bar form, jewellery and even scrap. The precious goods were then delivered to the Colombians offshore at their direction, who then resold the goods and the subsequent sale produced cash, which was unconnected with the original drug proceeds. According to US law enforcement this gold trade had become "the money laundering mechanism of choice," and was being used to wash "staggering amounts" of dirty money. US authorities prosecuted the owners of these Panamanian Jewellers in 2002 for money laundering which resulted in forfeiture to the US government of more than US\$40mio worth of gold, silver and other jewellery.

Country: Panama, US

Key date: 2002 (start of US prosecution for money laundering)

Beacon Hill

Beacon Hill Service Corporation was an unlicensed money services business based in NYC, with 12 employees. The US government has warned that Money Services Businesses are commonly used by money launderers. A Money Services Business in the US may collect several transmittal orders for small amounts from different individuals wanting to send money to relatives abroad. The Money Services Business then bundles them into a single transmittal order to a US bank as part of a transmittal of funds to a foreign Money Services Business. The single transmittal order does not identify all transmitters or recipients of the underlying order.

The US bank simply sends the single transmittal order to the foreign bank which then pays the foreign Money Services Business which then pays the foreign recipients based on the separate transmittal orders received directly from the US Money Services Business and vice versa.

From 1997-2003, Beacon Hill moved US\$6.5bio by wire transfers through numerous accounts it maintained at amongst others, J.P. Morgan Chase in Manhattan that ignored numerous red flags for money laundering, according to the Manhattan D.A.'s office. Beacon Hill moved money for clients who clearly preferred to operate clandestinely or under the radar.

Beacon Hill's client base included numerous offshore shell corporations and doleiros, or exchange houses, in Brazil and Uruguay, with most money coming from Latin America and transiting to the US or to third countries for example records show that Beacon Hill transmitted US\$31.5mio to accounts in Pakistan, Lebanon, Jordan, Dubai, Saudi Arabia and elsewhere in the Middle East. Wire transfer documents often identified the ultimate beneficiaries of transfers only as a "customer", one transfer of US\$100mio was attributed only to a "valued customer."

A large portion of Beacon Hill's business was run out of a pooled account that served many customers, making it impossible to link deposits with transfers out of the account. Despite concerns, that transfers could be linked to drug trafficking, only one such transaction valued at US\$25mio was identified.

Country: US

Key date: 2004 (convicted of operating as a money remitter without a licence)

Lespan

During the investigation of Beacon Hill (see above for more details) by the Manhattan District Attorney's Office concern over Lespan SA ("Lespan"), a money transmitter in Uruguay since 1976 arose, and in particular its connections to multiple Brazilian money service businesses transferring billions of US Dollars through Lespan's account at one of Bank of America's ("BoA") Manhattan branches.

The US investigation was conducted over two years, in which it was revealed that from May 2002 to April 2004, over US\$3bio flowed through Lespan's account at BoA. The case was a collaborative effort between US and Brazilian authorities. In the US, a joint investigation with ICE (Immigrations and Customs Enforcement), New York State Banking Department and Manhattan District Attorney's office led to the indictment of 34 people and 16 British Virgin Island companies for conducting illegal money transfer businesses in New York. Brazilian Federal Police executed over 121 arrest warrants and 215 search-and-seizure warrants in Brazil for money laundering and related tax evasion crimes.

Money exchange houses, or doleiros as they are known in Brazil, were able to exchange foreign currency but were

prohibited to send funds abroad. Lespan facilitated money transfers without proper documentation or registry with Brazil's central bank. For additional fees, Brazilian clients were able to move money in and out of Brazil without reporting to the government, by simply utilising services provided by doleiros. The illegal transfer services provided by the doleiros, allowed clients to have undeclared assets transferred without any reporting to Brazilian tax authorities. The elaborate scheme required the doleiros to have complex corporate structures whereby they had various related offshore accounts in the Caribbean and used Lespan to transfer clients' money anonymously. Similar to Beacon Hill, the Lespan accounts were utilised to facilitate payments to the Middle East via the Tri-Border region of Argentina, Brazil, and Paraguay. Historically, this area of South America has a strong connection to the Middle East due to a large concentration of its population of Middle Eastern origin. Billions of dollars are known to have flowed through the region and some of the monies may have gone to potentially fund terrorist activities.

Due to poor record keeping; it is difficult to really assess the potential impact that it may have had in funding terrorist activities around the world though it is unlikely to be substantial and in fact there was no specific evidence in this direction. Investigators noted too often it encountered cases where the money trail ceased and the ultimate recipient of the funds were never identified. Lespan, through its vast network of accounts at various banking institutions, kept its client identities to a minimum. Since the corresponding banks did not question the flow of funds, it simply remained undetected for years.

Key date: 2004 (actions announced over Uruguayan money transmitter making US\$3bio)

Special Focus 25 **Pedro Alatorre**



Casa de Cambio Puebla was founded in 1985 and licensed by Mexican banking regulators. It had 17 branch offices throughout Mexico and employed 240 people. In order to process transactions it maintained 46 correspondent accounts at Wachovia (now part of Wells Fargo) branches in Miami and New York. One of the larger branches of Casa de Cambio Puebla operated out of the Mexico City Airport and was run by Pedro Alatorre. Alatorre used the Branch to launder drug monies for the Mexican "Pacific Cartel" headed by notorious fugitive Joaquin "el Chapo" Guzman Loera (see Mexican Gangs Part 2, Section 5 above), for whom Alatorre worked.

It is believed that couriers carrying clear plastic bags stuffed with cash went to the Airport branch. Alatorre then arranged for monies to be deposited into accounts opened at HSBC in Mexico. These accounts had been set up by Alatorre using the stolen identities of 74 people. Once in the HSBC accounts in the names of Companies controlled by Alatorre, for example Grupo ETPB SA and Grupo Ráhero SC, the monies could be used by the drug traffickers to finance their operations, for example by purchasing planes in the US to be used for air transporting cocaine from Latin America into Mexico before being moved overland into the US.

One such purchase was of a DC-9 in early 2006 sold by US Oklahoma City Aircraft broker, US Aircraft Titles Inc. Funds controlled by Alatorre in Mexico were wired to the correspondent account of Casa de Cambio Puebla at Wachovia in Miami and from their Wachovia wired the funds (approx US\$300,000) at the instruction of Alatorre to an account at Bank of America from which the sale was concluded. The link to the Wachovia accounts and the link to the Casa de Cambio Puebla, came from a 2006 cocaine seizure in Mexico. On 5 April 2006, a pilot working for mexican drug traffickers flew the same DC - 9 aircraft from Florida to Caracas in Venezuela, picking up 5.7 tons of cocaine. The drugs were packed into 128 black suitcases and valued at US\$100mio. The drugs were then to be flown to Mexico, where they would be collected and then smuggled into the US overland. On 10 April Mexican authorities seized the plane once it landed in Ciudad del Carmen in Mexico, 500 miles east of Mexico City. Once the drugs were seized and destroyed and those caught in the smuggling operation arrested and charged, investigators began looking at how the aircraft was owned and how its purchase had been financed in order to try to net additional suspects involved and connected with the drug trafficking operation. Working backwards it was then that the links to Wachovia and Puebla and Alatorre were established.

On 16 May 2007, DEA agents conducted a raid of Wachovia's international banking offices in Miami, with orders to seize Puebla's accounts. With Puebla's Wachovia accounts seized, Alatorre and his partners shifted their laundering scheme to HSBC in Mexico. In the three weeks after the DEA raided Wachovia, Grupo ETPB SA and Grupo Ráhero SC, made 12 cash deposits totalling US\$1 mio at an HSBC Mexican branch. The funds financed a Beechcraft King Air 200 plane that police seized on 29 December 2007, in Cuernavaca, 50 miles south of Mexico City. Mexican Authorities would seize two more airplanes by following the money trail left by Casa de Cambio Puebla via Wachovia. Each of Casa de Cambio Puebla, Alatorre and three other employees were indicted in Miami in February 2008 for drug trafficking and money laundering. In May 2008, the extradition of the suspect was sought alleging they used shell firms to launder US\$720mio through US banks. Alatorre has been in a Mexican jail for 2 1/2 years.

Penalty: Imprisonment in a Mexican Jail
Actions: laundered Mexican drug cartel cash via position as head of Mexican Casa de Cambio branch)

Country: Mexico, US
Key date: 2006 (Cocaine seizure by US authorities then led to link to the MSB, Wachovia and HSBC)

Goods Traffickers

Operation Pangea and Others

In the last few years, Interpol has spearheaded Operations to combat the trafficking of counterfeit and pirated goods, in particular; Operation Pangea (2009); Operation Jupiter V (2010); Operation Atlantique (2010); Operation Opson (2011); and Operation Maya (2010).

Operation Pangea

Operation Pangea was an international week of action tackling the online sale of counterfeit and illicit medicines and highlighting the dangers of buying medicines online. The annual operation brought together customs, health regulators, national police and the private sector from countries around the world. Activities targeted the three principal components used by illegal websites to conduct their trade – the Internet Service Provider (ISP), payment systems and the delivery service.

The operation gained significant momentum since its launch in 2008. The first phase of the operation brought together 10 countries, with the number rising to 100 in 2012. In 2012, 3.75 million illicit and counterfeit pills were confiscated at an estimated value of US\$10.5mio. More than 18,000 websites were shut down. Some 133,000 packages were inspected by regulators and customs authorities, of which around 6,700 were confiscated. Eighty individuals were under investigation or under arrest for a range of offences, including operating a clandestine laboratory producing counterfeit medicines; membership of a criminal group selling illicit medicine online; and operating websites selling illicit medicines.

Country: Australia, Canada, Germany, Ireland, Israel, New Zealand, Singapore, Switzerland, UK and US of America and many more.

Key date: 2008-2012 (annually)

Operation Jupiter V

Launched in 2004, Operation Jupiter expanded in scope every year. Each phase of the operation targeted an increasingly wide range of counterfeit and illicit goods, in more distribution channels and in more countries. Operation Jupiter V (2010) resulted in the seizure of nearly 8 million counterfeit products worth more than US\$200mio and led to nearly 1,000 arrests.

Seizures have highlighted the dangers that counterfeit products pose to public safety. Car parts, motor oil and construction materials, such as powders to make concrete and glue, were examples of new commodities seized under Jupiter V. These unregulated goods were generally sub-standard and so constituted a major risk to the population at large. Other types of goods recovered included sports clothes and shoes, sunglasses, mobile phones, books, car parts, computer software and alcohol. Goods were recovered from a range of locations including markets, commercial shopping centres and from street vendors, and in a number of cases social networking sites were also identified as distribution channels for counterfeit products.

Ilicit goods infiltrated well-known shopping centres while luxury items appeared for sale on Internet social networks. Operation Jupiter focused on these goods in a variety of outlets including at sea, to detect the routes used by boats smuggling illegal goods. Operation Jupiter was led by Interpol in partnership with the World Customs Organisation (WCO).

Country: Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, France (French Guyana), Panama, Paraguay, Peru, Suriname, Uruguay and Venezuela

Key date: 2010

Operation Atlantique

Operation Atlantique was an Interpol led initiative to combat counterfeiting and all types of illicit trade across Western Africa. The action in 2011 resulted in 16 arrests and the seizure of fake products worth more than US\$1.5mio. In addition to conducting raids on wholesalers and markets in the city centres of Lomé, Togo and Accra, Ghana, officers also carried out checks and seizures at the seaport of Tema in Ghana, one of the key entry points for merchandise in Western Africa. Recovered products included soup cubes, computer supplies, African fabrics, plastic packaging used for food and water, cigarettes and CDs.

Country: Benin, Burkina Faso, Ghana, Nigeria and Togo.

Key date: 2011

Operation Opson

Hundreds of tonnes of fake and substandard food and drink including champagne, cheese, olive oil and coffee were seized in an Interpol/Europol coordinated operation across 10 countries, effectively disrupting the organised criminal gangs behind this high profit-low risk activity which undermines legitimate business and puts the safety of consumers at risk. Operation

Opson (meaning food in ancient Greek) resulted in the recovery of more than 13,000 bottles of substandard olive oil, 30 tonnes of fake tomato sauce, around 77,000 kg of counterfeit cheese, more than 12,000 bottles of substandard wine worth EUR 300,000, five tonnes of substandard fish and seafood and nearly 30,000 counterfeit candy bars. The sale of fake/substandard caviar via the internet was also under investigation. The operation saw checks carried out in airports, seaports, shops and flea markets across the 10 participating countries. Consumers buying these goods, either knowingly or unknowingly, are putting their health at risk as the counterfeit food and drink are not subject to any manufacturing quality controls and are transported or stored without proper regard to hygiene standards.

Country: Bulgaria, Denmark, France, Hungary, Italy, The Netherlands, Romania, Spain, Turkey and the UK.

Key date: 2011

Operation Maya

Operation Maya saw more than 1,000 interventions and more than a million items recovered by Authorities in the Americas at key locations such as land, sea and airport border control points in addition to markets, shops and street vendors. Two hundred individuals were arrested or were under investigation for related criminal offences. Fake goods including toys, computer software, clothing, beauty products, engine oil and cigarettes worth nearly US\$30mio were seized in this Interpol-coordinated operation. The operation also revealed increasingly elaborate efforts by criminals to avoid detection, with items smuggled into a country via one route, while counterfeit trademark materials including stickers for computers, batteries, mobile phones and even car emblems were sent separately to be used later to 'brand' the products. Operation Maya again showed that there is no product which is not being counterfeited and criminals are using every means available to traffic fake and illicit goods.

The operation has again shown the importance of cooperation and coordination among police, customs, prosecutors and the private sector to combat organised crime in all participating countries.

Country: Belize, Canada, Colombia, Costa Rica, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama and US.

Key date: 2012

Human Traffickers

Robert Mikelsons

Robert Mikelsons a Dutch national was sentenced to 12 years in prison for abusing more than 60 children, some just a few months old, in two Amsterdam nurseries and homes where he worked. Mikelsons, took explicit pictures and shared these with other pedophiles on the Internet. US and Dutch police cooperation using Interpol tools broke the case. US Immigration and Custom Enforcement (ICE) and Homeland Security Investigations (HSI) shared seized child sexual abuse images with specialist investigators worldwide via Interpol who added the images of the sexual abuse of an 18-month-old to Interpol's International Child Sexual Exploitation (ICSE) database. As a result a specialist Dutch police officer who is a member of Interpol's Victim Identification Network in the Netherlands, identified a stuffed bunny in the photo as 'Miffy', a character in Dutch children's books. The toy, in addition to other elements in the image, enabled the KPLD Dutch National Police to identify the Netherlands as the location where the photos of the child sexual abuse had been taken. A public appeal by the Dutch police on national television resulted in the identification and arrest of Robert Mikelsons.

Subsequent investigations around the world have so far led to the arrest of nearly 40 sex offenders from every region of the world, many of them abusing multiple victims. To date, the number of children removed from harm as a result of this one operation stands at more than 140.

According to Ron Noble, the Head of Interpol, "This is exactly why we created the Interpol International Child Sexual Exploitation database. It is a vital weapon for law enforcement officers in bringing dangerous criminals to justice, and should be the first port of call for any investigation into child sexual abuse." Managed by Interpol's Crimes Against Children specialist unit at its headquarters in Lyon, France, the ICSE database, backed by the G8 and funded by the European Commission, is accessible to victim identification specialists through Interpol's secure I-24/7 global police communications system, and uses sophisticated image comparison software to make connections between victims and places. The database contains images relating to nearly 2,500 identified victims of sexual exploitation from 41 countries, and in addition to providing vital assistance in locating offenders, is also an important tool in avoiding duplication of effort by police trying to identify victims who have already been rescued.

Country: Netherlands and elsewhere

Key date: 2012 (child sex abuser jailed, leading to rolling up on international sex ring)

Operation Bia and Others

In the last few years, Interpol has spearheaded Operations to combat child abuse in Africa, in particular;

Operation Bia (2009); Operation Cascades (2010); Operation Bana (2010); and Operation Bia II (2011);

Operation Bia

54 suspected child trafficking victims from 7 different countries were identified and taken into care and 8 individuals arrested following an operation led by police in Côte d'Ivoire in cooperation with Interpol, in the first ever police operation targeting child trafficking in West Africa. Police simultaneously targeted a selection of plantations believed to be using illegal child labour. In addition, vehicles travelling on the main roads leading from Ghana were systematically checked for potential child victims. Codenamed 'BIA' after the river which separates Ghana from Côte d'Ivoire. The 54 children had been bought by plantation owners needing cheap labour to harvest the cocoa and palm plantations. They were discovered working under extreme conditions, forced to carry massive loads seriously jeopardizing their health. Aged between 11 and 16, children told investigators they would regularly work 12 hours a day and receive no salary or education. Girls were usually purchased as house maids and would work a seven-day week all year round, often in addition to their duties in the plantations.

With Ghana and Côte d'Ivoire producing around three quarters of the world's cocoa, it is believed that hundreds of thousands of children are working illegally in the plantations across these two countries alone. The trafficking of children is often camouflaged by the cultural practice of placing young children with families of wealthier relatives to receive an education or learn a trade. In reality, they are often sold and their rights to education, health and protection denied.

Country: Côte d'Ivoire

Key date: 2009 (54 trafficked/abused children rescued in police operation supported by Interpol)

Operation Cascades

More than 100 suspected child trafficking victims were identified and taken into care and 11 individuals arrested following an operation led by police in Burkina Faso and supported by Interpol. Dozens more children have also now been returned to their families following child labour investigations. Involving nearly 100 police officers, Operation Cascades took place across Burkina Faso's western Cascades region and in the capital Ouagadougou, and also included customs and environmental officers, non-governmental organisations, officials from the Ministries of Health and Social Affairs, and prosecutors. During a three-day operation, police officers checked highways linking Burkina Faso's capital to other regions in the country and to adjoining

countries, and also raided illegally-operated gold mining quarries in the Cascades region. Authorities took 177 children into their charge, of which 103 suspected trafficked children were taken into care by social services, while another 74 were returned to their families as part of an awareness campaign against child labour. The initiative in Burkina Faso followed Operation Bia in Côte d'Ivoire which also targeted illegal child labour and resulted in the rescue of 54 children.

Country: Burkino Faso

Key date: 2010 (177 trafficked/abused children rescued in police operation supported by Interpol)

Operation Bana

140 victims of child trafficking and labour were rescued in the Gabon in an Interpol co-ordinated operation code-named Bana. The children from 10 different countries were forced to work as labour in local markets. During the operation, teams of officials carried out checks at market stalls in the capital city Libreville, where children as young as six years old were working in a variety of roles, from carrying heavy goods, to selling products. The children were taken into care and 44 people were arrested as a result.

Country: Gabon

Key date: 2010 (140 trafficked/abused children rescued in police operation supported by Interpol)

Operation Bia II

116 suspected child trafficking victims were identified and taken into care in Ghana being rescued from forced labour in the fishing industry along the country's Volta Lake area, in an operation coordinated by Interpol which also resulted in 28 arrests and convictions. The rescued children were aged between 5 and 17. Ghanaian Police teams along with Interpol agents simultaneously targeted selected fishing communities believed to be using illegal child labour. The 28 individuals arrested during the operation were sentenced to 16 months imprisonment each after the accused pleaded guilty to exposing children to danger and engaging minors in hazardous activities. The operation revealed that 15 of the rescued children had been trafficked from other regions of Ghana. A separate operation across Accra City also saw officers from a variety of law enforcement agencies interview 120 sex workers to determine if they were part of a wider human trafficking network operating in Ghana. As a result 29 of these were found to be minors who were being sexually exploited and were taken to shelters and housed by the authorities.

Country: Ghana

Key date: 2011 (116 trafficked/abused children

rescued in police operation supported by Interpol)

Operation Tuy

Nearly 400 suspected child trafficking victims were identified and taken into care and 73 individuals arrested following an operation led by police in Burkina Faso and supported by Interpol. Operation Tuy which targeted sites in Ougadougou, Houndé and Bobo Dioulasso, resulting in 387 children being discovered working under extreme conditions, lowered into narrow, airless mining holes up to 70 metres in depth, receiving no salary or education, with young girls often also subjected to sexual abuse. The victims have now been returned to their families or taken into care.

Country: Burkino Faso

Key date: 2011 (400 trafficked/abused children rescued in police operation supported by Interpol)

Terrorism Financiers

International Islamic Relief Organisation (IIRO) - Philippine and Indonesian branches

The IIRO is a Wahhabi sponsored charity. Established in 1978, it has branch offices throughout the world, including 36 in Africa, 24 in Asia, 10 in Europe and 10 in Latin America, the Caribbean and North America. The bulk of its financial contributions come from private donations in Saudi Arabia. This includes a long standing endowment fund (Sanabil al-Khair) established to generate a stable income to finance its various activities. The IIRO continues to be closely associated to the Muslim World League with which it participates in many joint activities. Many prominent Middle East figures and financiers have supported this mainstream Islamic charity. But, the IIRO has also, it is claimed, been used to channel funds to Al-Qaeda. According to a CIA report, funds raised through the IIRO were used to support at least six Al-Qaeda training camps in Afghanistan prior to 9/11. Evidence produced in Canadian Court proceedings also linked the IIRO directly to groups responsible for the 1998 bombings of the American Embassies in Dar es Salaam and Nairobi. The former head of the IIRO office in the Philippines, Muhammad Jamal Khalifa, was also accused of links to Al-Qaeda and terrorist activities. In 2006 US Treasury designated the Philippine and Indonesian branches only as supporters of terrorism.

Country: Saudi Arabia, Philippines

Key date: 1990s (contact with Al-Qaeda by a senior officer at IIRO affecting Philippine and Indonesian branches)

Special Focus 26 **Holy Land Foundation**



The Holy Land Foundation was the largest Islamic charity in the US. Established in California in 1989 and later in 1992 headquartered in Texas. It had offices in California, New Jersey, and Illinois, and individual representatives scattered throughout the US, the West Bank, and Gaza. It was originally known as Occupied Land Fund. In 2007, US federal prosecutors brought charges against the organisation for funding Hamas and other "Islamic terrorist organisations".

The 2008 trial of the charity leaders was dubbed the "largest terrorism financing prosecution in American history." In 2009, the founders of the organisation were given life sentences for "funnelling US\$2mio to Hamas. The organisation's website stated: "Our mission is to find and implement practical solutions for human suffering through humanitarian programmes that impact the lives of the disadvantaged, disinherited, and displaced peoples suffering from man-made and natural disasters." Their primary area of focus was with the Palestinian refugees in Jordan, Lebanon, and the Palestinian Territories. They also provided support to victims after disasters and wars in Bosnia, Kosovo, Turkey, and the US (after Iowa floods, Texas tornadoes, and the Oklahoma City bombing).

Among the founders of the Holy Land Foundation was Mousa Mohammed Abu Marzook, a political leader of Hamas, who provided substantial funds to the Holy Land Foundation in the early 1990s. In 1994, Marzook (who was named a Specially Designated Terrorist by the Treasury Department in 1995) designated HLF as the primary fund-raising entity for Hamas in the US. He was deported from the US to Jordan in 1997. Marzook was indicted on 20 August 2004, by a US federal grand jury in Chicago. He and two other individuals were charged with a 15-year conspiracy to raise funds for terrorist attacks against Israel. In the year 2000 alone, HLF raised over US\$13mio.

According to the US Department of Treasury, HLF supported Hamas activities through direct fund transfers to its offices in the West Bank and Gaza that are affiliated with Hamas, and transfers of funds to Islamic charity committees ("Zakat Committees") and other charitable organisations that are part of Hamas or controlled by Hamas members. The Department of Treasury also reported that HLF funds were used by Hamas to support schools that served Hamas' ends by encouraging children to become suicide bombers and to recruit suicide

bombers by offering support to their families. Edward Abington, former US Consul General in Jerusalem, acted as a defence witness and testified that during his daily CIA briefings he had never been informed that Hamas controlled the Palestinian charity groups mentioned.

In December 2001, the assets of the organisation were frozen by the FBI and Treasury agents. Treasury officials conceded that whilst a "substantial amount" of the money raised went to worthy causes, but insisted that Holy Land's primary purpose had been to subsidise Hamas. Repeated appeals to the courts by the Holy Land Foundation to have the freeze lifted failed.

On 27 July 2004, a federal grand jury in Dallas, Texas, returned a 42-count indictment against the Holy Land Foundation. Charges included: conspiracy, providing material support to a foreign terrorist organisation, tax evasion, and money laundering. The indictment alleged that the Holy Land Foundation provided more than US\$12.4mio to individuals and organisations linked to Hamas from 1995 to 2001, when their assets were frozen. The indictment also named specific seven top officers of the Holy Land Foundation: Five of the seven were arrested, the remaining two have not been found, and are considered fugitives. In December 2004, a federal judge in Chicago ruled that the Holy Land Foundation (along with the Islamic Association of Palestine and the Quranic Literacy Institute) was liable in a US\$156mio lawsuit for aiding and abetting the militant group Hamas in the death of a 17-year-old American citizen named David Boim.

A Holy Land Foundation criminal trial began on 23 July 2007, in Dallas, Texas. It was claimed during the 2007 trial that the Justice Department fabricated quotes and modified transcripts. Critics faulted much of the evidence given during the trial. The New York Times said Israeli agents using pseudonyms testified for the prosecution. The government did not allege that the foundation paid directly for suicide bombings, but instead that the foundation supported terrorism by sending more than US\$12mio to charitable groups, known as Zakat Committees, which build hospitals and feed the poor. The prosecution said the committees were controlled by Hamas, and contributed to terrorism by helping Hamas spread its ideology and recruit supporters. Some of these charitable committees were still receiving US funding through the USAID programme as late as 2006.

After 19 days of deliberations, the 2007 jury was unable to come to a definitive conclusion and the case ended in a mistrial. While 200 charges were filed against the defendants, the jurors had acquitted on some counts and were deadlocked on charges ranging from tax violations to providing material support for terrorists. One defendant was acquitted of most of the 32 charges against him. The federal government began a retrial on August 18, 2008.

On 24 November 2008, the government obtained guilty verdicts against the Holy Land Foundation and five individual defendants in the retrial.³⁷ Holy Land was found guilty of giving more than US\$12mio to support the Palestinian militant group Hamas, which the US designated as a terrorist organisation in 1995, and made supporting the group illegal. Two of the guilty received each 65 years imprisonment. The jury found against the Holy Land Foundation on all 108 charges. The charges included conspiracy to provide material support to a foreign terrorist organisation, providing material support to a foreign terrorist, and conspiracy to commit money laundering. "Today's verdicts are important milestones in America's efforts against financiers of terrorism", Patrick Rowan, Assistant Attorney General for National Security, said after the trial. "This prosecution demonstrates our resolve to ensure that humanitarian relief efforts are not used as a mechanism to disguise and enable support for terrorist groups."

Country: US, Palestinian Territories
Key date: 2001 (assets frozen and later conviction secured for providing material support (US\$12mio) to Hamas)

The Benevolence International Foundation (BIF)
The Benevolence International Foundation is another Saudi umbrella charity organisation that has served as an important funding source for Al-Qaeda. BIF was established in the late 1980's as two separate organisations. One, the Islamic Benevolence Committee was established as a charity based in Peshawar, Pakistan and Jeddah, Saudi Arabia. Its titular founder was Sheikh Adil Abdul Batarjee.

Its sister organisation, Benevolence International Corporation was set up as an import export business in the Philippines by Mohammed Jamal Khalifa, who also headed the Philippines IIRO office.

Both organisations were engaged in raising funds to support the mujahideen in Afghanistan. The two organisations appeared to work separately until the early 1990s. In 1992 they became the Benevolence International Foundation and opened new branches throughout Southeast Asia as well as in Europe and America.

The US Treasury Department took action in December 2001 to designate BIF as financiers of terrorism. The US subsequently called upon the Security Council to add BIF to its consolidated list of entities associated with Al-Qaeda. The Treasury Department charged that BIF and its chief executive officer, Enaam Arnaout were involved in funding Al-Qaeda activities including "the purchase of rockets, mortars, rifles and offensive and defensive bombs, and ... (distributing) them to various mujahideen camps, including camps operated by Al-Qaeda." The Treasury document also cited direct links between Arnaout and bin Laden, and with Mamdouh Mahmud Salim, a bin Laden lieutenant.

Country: Saudi Arabia, Pakistan, Philippines
Key date: 2001 (US Treasury designate as terror financing charity)

Muwafaq Foundation or "Blessed Relief"
Muwafaq Foundation or "Blessed Relief" charity was established in 1991 by Yassim al-Qadi. The stated purpose of the charity was to "relieve disease, hunger and ignorance." The Charity was active in Bosnia during the Balkan wars and was closed in 1998 following allegations of fundraising and transferring of funds on behalf of Al-Qaeda and other terrorist organisations. The foundation's principal benefactor was Khalid Bin Mahfouz. Al-Qadi was subsequently designated by the US Treasury Department on October 12, 2001 as well as the UN, the EU and others. Yassim al-Qadi has always protested his innocence and challenged his listing which has been accepted and he has been removed from the UN, EU and some other lists though not the US.

Country: Saudi Arabia, Bosnia
Key date: 2001 (Al-Qadi designated by US and others as a terrorist financier, later designation lifted except by US)

Al-Rashid Trust
The Al-Rashid Trust (ART) was founded by Mufti Mohammed Rashid in 1996, in Karachi, Pakistan, which coincided with the Taliban coming to power in neighboring Afghanistan. The Trust gradually grew to operate 21 branches across Pakistan but also in Afghanistan.

Described as a 'welfare organisation', one of its original charters was to carry out welfare projects within Pakistan, with financial resources provided by public donations. Overtime, the ART expanded its mandate to carry out 'relief activities' for Muslims in Chechnya, Kosovo and Afghanistan.

The ART shares a similar religious ideology with that of the Taliban and has promoted "jihad" at times, for example with statements in ART booklets such as "the holy war is an essential element of Islam," and "any Muslim must carry the weapons, even with the mosque, if the need would be felt to make fire on a non-Moslem."

ART literature also denounces the US for its policies toward Israel, Iraq and Saudi Arabia and praises Islamist terrorists. Among the other ART objectives is providing assistance to 'illegally jailed' Muslim prisoners.³⁸

The trust runs many madrassas and mosques in Pakistan including the largest Arabia-Islamia in Mansehra.

The network of ART aided madrassas in Pakistan reportedly act as recruiting centres for Jihadis. It also runs a hospital in Muzaffarabad in Pakistan occupied Kashmir (PoK) for the treatment of injured terrorists.

Mufti Rashid has been reported to have had direct

access to Osama bin Laden and the Taliban. The Al-Rashid Trust is also closely linked with Jaish-e-Mohammed and other terrorist outfits active in India's Jammu and Kashmir.

Al-Rashid documents indicate that the Trust secures most of its finances from zakat (annual alms) and overseas donations, particularly from the Middle East and Pakistan, but also from a network in South Africa. However, the sources of donation are kept secret.

The trust was one of a number of groups and organisations listed by the US State Department on September 22, 2001, for involvement in financing and supporting a network of international Islamist terrorist groups, a claim denied by the trust.

Country: Pakistan, Afghanistan
Key date: 2001

The Rabita Trust
The Rabita Trust was established in Pakistan in 1988 ostensibly to repatriate and rehabilitate stranded Pakistanis from Bangladesh. Its stated aims included the dissemination of Dawah (culture), to expound the teachings of Islam, "and to 'defend' Islamic causes in a manner that safeguards the interests and aspirations of Muslims. Most of its funding was secured from Saudi businessmen.

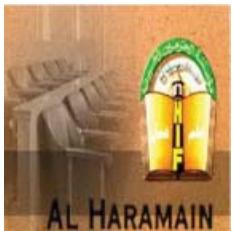
Funds from the trust were reportedly used for a number of Al-Qaeda related activities, including recruitment and training in Afghanistan, Pakistan and elsewhere. The Rabita Trust was run by Wael Hamza Julaidan, who the US Treasury Department charged was an associate of bin Laden and Ayman al-Zawahiri. He was designated by the US and the UN as an Al-Qaeda associate in late 2002.

The US administration has pointed out that the Rabita Trust is part of a web of charities funding Islamist terrorist movements such as bin Laden's Al Qaeda network. Whilst disputed by those running the Trust and by those also designated as terrorist fundraisers by the US including Pakistani based Al-Akhtar Trust, and the Al-Rashid Trust.

Country: Pakistan, Saudi Arabia
Key date: 2002 (Julaidan designated by US and UN as terrorist financiers)

Special Focus 27

Al Haramain Islamic Foundation (Bosnian & Somalian offices)



Charity forms a very important part of Muslim law and tradition. There is a recognised religious duty in the Muslim world to provide a set portion of ones earnings or assets for religious or charitable purposes (Zakat), and otherwise to support charitable works through voluntary deeds or contributions (Sadaqah). In countries like Saudi Arabia or the United Arab Emirates that have no established income tax system, the Zakat substitutes as the principal source of funding for religious, social and humanitarian organisations and activities. The funds are collected by the Government, or though local mosques and religious centres. Sadaqah contributions are also made directly to established Islamic charities.

As both Zakat and Sadaqah are viewed as personal religious responsibilities there has traditionally been little or no government oversight of these activities. Donations in large measure remain anonymous. Al-Qaeda and other terrorist Groups have taken full advantage of this lack of oversight to open its own front charities and to solicit funds through collection boxes at mosques and Islamic centres. It has also placed operatives in key positions within established charities that are able to do its bidding.

Funds raised or allocated by or for Al-Qaeda are co-mingled, maintained and transferred with funds designated for legitimate relief Al-Qaeda and developmental activities. Their ultimate use to support Al-Qaeda activities can only become known when the moneys are transferred or diverted to Al-Qaeda-related recipients.

The Al Haramain Islamic Foundation based in Jeddah, is one of Saudi Arabia's most active charities in spreading Islamic teachings. Al Haramain reportedly funded some 3000 Wahhabi missionaries and concentrated heavily in establishing new Wahhabi Mosques in Southeast Asia, the Balkans, and Africa. Since 9/11, Al Haramain has come under close international scrutiny as a possible conduit for Al-Qaeda funding. According to its web site, Al Haramain operates in some 49 countries. It raises some US\$30mio per year drawing its funding largely from Saudi donors. Its founding general manager Sheikh Aqeel al-Aqeel maintained a close relationship

with the Saudi Ministry of Islamic Affairs, and the Saudi government was considered one of its principal benefactors. On 11 March 2002, the US and Saudi Arabia jointly designated the Bosnia and Herzegovina and Somalia offices of Al-Haramain as an Al-Qaeda funding source.

Al-Haramain Somalia had funneled money to Al-Ittihad al-Islami, a designated terrorist group, by disguising the funds as contributions for an orphanage project and for Islamic school and mosque construction. The Bosnia office was linked to Al-Jemaah al-Islamiyah al-Masriyah and to bin Laden. Further investigations also implicated branches in Albania, Croatia, Ehtiopia, Kenya, Kosovo, Indonesia, Pakistan, and Tanzania. The Russian government has also complained to Saudi Arabia regarding alleged Al Haramain funding for Chechen rebels. The Saudi government has removed Sheikh Al-Aqeel as Al Haramain's General Manager and ordered the closing of 15 branches outside Saudi Arabia. Sheikh Aqeel al-Aqeel was designated by the US Treasury in June 2004 and his name was added to the UN's Al-Qaeda associate list.

Country: Saudi Arabia, Bosnia, Somalia
Key date: 2002 (Saudi and US jointly designate Bosnian and Somalian offices as Al-Qaeda funding sources)

The Afghan Support Committee/Revival of Islamic Heritage Society

The Afghan Support Committee (ASC) was a non-governmental organisation based in Afghanistan, established by bin Laden and affiliated with the Revival of Islamic Heritage Society, both raised money for Al-Qaeda from local Arab non-governmental organisations by claiming the funds were for orphans and widows. Both were listed by the UN in 2002 for participating in the financing and planning, as well as assisting in the facilitation of terrorist acts.

Country: Afghanistan
Key date: 2002

Global Relief Foundation, Taibah International and Al Furqan

The Global Relief Foundation (GRF) initially operated in Bosnia and Herzegovina as a non governmental organisation under the umbrella of Taibah International, but then in 1996, Taibah broke with GRF, but continued to share the same office in Sarajevo, Bosnia and Herzegovina, as did another non governmental organisation, Al Furqan. The groups were listed between 2002 and 2004 by the UN as having close ties to Al-Qaeda and to the Bosnian branch of Al-Haramain Foundation.

Country: Bosnia and Herzegovina
Key date: 2002-2004

Special Focus 28

Interpal & Others



On 22 August 2003 the US Treasury announced the designation of five alleged Hamas related charities and six senior Hamas leaders as Specially Designated Global Terrorists (SDGTs),³⁸ freezing any assets in the US and prohibiting transactions with US nationals. This followed

on from a spring and summer terror rampage in 2003 by Hamas who took responsibility for ten different terrorist attacks that occurred in Israel between 27 March 2002 and 19 August 2003. The attacks included killings of civilians in suicide bombings and shootings in Israel during this time. "By claiming responsibility for the despicable act of terror on 19 August, Hamas reaffirmed that it is a terrorist organisation committed to violence against Israelis and to undermining progress toward peace between Israel and the Palestinian people," President Bush stated. "Hamas' leaders and those who provide their funding again have the blood of innocents on their hands," US Treasury Secretary John Snow stated. "Empty words cannot wash them clean. As they resist the road map for peace, Hamas is devastating the dreams of the Palestinian people for freedom, prosperity, and an independent state."

The US Treasury then listed a number of individuals and the following charities that they claim provide support to Hamas and form part of its funding network in Europe: Comité de Bienfaisance et de Secours aux Palestiniens (CBSP), of France, the Association de Secour Palestiniens (ASP), of Switzerland. (An organisation related to CBSP), the Palestinian Relief and Development Fund, or Interpal, headquartered in the UK, the Palestinian Association in Austria, PVOE and the Sanabal Association for Relief and Development, based in the Lebanon. The US Treasury stated that: "today's action follows several actions taken against Hamas previously, including the designation of several entities that formed part of the Hamas network such as Holy Land Foundation for Relief and Development and the Al Aqsa Foundation, key sources of financial support for Hamas."

Following these designations a number of lawsuits followed from those injured or those related to victims of Hamas terrorist acts. These civil liability claims seek treble damages under the US Anti Terrorism Act of 1992 ('ATA'). The ATA has extra territorial jurisdiction and so there is no need for there to be a connection to the US in relation to the alleged criminal acts or the financial transactions: It is sufficient for a claim to be made if the

Plaintiffs are US nationals, or the heirs or survivors of US nationals. It is not material also if transactions are other than in US\$. Nat West (now part of Royal Bank of Scotland Group) is a UK based financial institution with offices around the world and including in the US. The Complaint alleges that for more than 9 years Nat West knowingly maintained numerous accounts in dollars, euros and pounds for the charity Interpal (Interpal was first suspected of channelling money to Hamas in 1996; (Israel designated it a terrorist organisation in 1998 and the US designated it in 2003). For more details see Part 1, Section 3, Sanctions and Embargoes above. The Complaint further alleges that Nat West transferred and received money between these Interpal accounts and various alleged terrorist organisations with links to Hamas, namely the Jenin Committee, Tulkarem Committee, Holy Land Foundation and Al-Aqsa Foundation. The Complaint alleges 6 specific occasions on which Nat West supposedly accepted deposits or made transfers on behalf of Interpal involving alleged terrorist organisations. The plaintiffs further allege that Hamas receives most of its funding through donations coordinated by a global network of charities known as the Union of Good operated by the Muslim Brotherhood. The Union of Good is comprised of more than 50 Islamic charitable foundations worldwide including the Palestinian Relief and Development Fund ('Interpal').

At a hearing of the bank's petition to dismiss the lawsuit the Judge granted the dismissal in relation to one claim that the bank had aided and abetted the murder, attempted murder and serious bodily injury of American nationals, but denied the dismissal in respect of the other two claims that the bank knowingly provided material support or resources to foundations including the Al Aqsa Foundation, a key source of financial support for Hamas.

On 28 March 2013 the Eastern District Court granted summary judgment to NatWest finding that the plaintiffs had failed to establish sufficient evidence to prove that NatWest either "had actual knowledge" that Interpal was funding Hamas" or had acted with "exhibited deliberate indifference." In assessing the banks state of mind, the Judge noted the banks compliance with foreign banking laws. This decision has been appealed.

Carnival French Ice-Cream

Carnival French Ice Cream Supermarket based in Brooklyn, New York and owned by a nationalised Yemenite, looked to many as a straightforward ice cream parlor. Tax records showed Carnival had average annual receipts at approximately US\$185,000 per annum. In fact prosecutors believed it took in approx US\$22mio between 1996 and 2003 with the monies flowing through the Carnival accounts in favour of Islamic causes. Abad Elfgehl began informally sending money for family and friends to Yemen for a fee in 1995. He claimed he intended to get a license but never got around to it. His unregulated money transfer business then expanded to service amongst others locals

who frequented his local Brooklyn Mosque (Al Farook Mosque - which was also the place of worship for the men involved in the 2003 WTC bombing). The locals would fund the Carnival business account with regular wire transfers from accounts established by them and styled as small business accounts. All feeder payments were below the US currency transaction reporting limit of US\$10,000. Once the funds were received in the Carnival account, and consolidated, the majority of the funds were wire transferred to individuals, companies and Banks in Saudi Arabia, Yemen, the UAE, Thailand, China and Canada. Initially Abad Elfgeeh was arrested in late 2003 for laundering money for Islamic Terrorism, not it appears from any alert or suspicious activity report filed by the bank handling the monies but following the arrest and interrogation of Al - Moyayad, where monies received by Al-Moyayad in Yemen were traced back via Carnival and to the Mosque. In early 2006 Elfgeeh was convicted of illegally transferring money overseas, but the terror link was dropped as prosecutors realised they could not prove a terror connection. He was nevertheless imprisoned for 15 years.

Country: US, Yemen and elsewhere

Key date: 2003 (arrested and charged with terror offences)

al-Aqsa Foundation

The al-Aqsa Foundation was an international charity, which described itself as an Islamic social aid institution financially supporting various organisations in Israel, the West Bank and the Gaza Strip involved in humanitarian emergencies, with its head office located in Germany with branch offices in the Netherlands, Denmark, Belgium, Sweden, Pakistan, South Africa, Yemen and elsewhere. In May 2003 the al-Aqsa Foundation was effectively shut down, first designated by the US as a terrorist entity and soon afterwards by other nations, including the Netherlands, Germany, Denmark, the United Kingdom, Luxembourg and Switzerland, freezing funds and financial assets in the foundation, because (according to the US it was a "critical part of Hamas' transnational terrorist support infrastructure" and that it "uses humanitarian relief as cover to provide support to the Hamas terrorist organisation." Hamas is known to raise at least tens of millions of dollars per year throughout the world using charitable fundraising as cover.

Country: Europe, Israel/Palestinian Territories
Key date: 2003

Al-Akhtar Trust

The Al-Akhtar Trust (AAT) was formed in Karachi, Pakistan in November 2000 to provide financial assistance for Islamist extremists, including the Taliban and to feed, clothe and educate the children of religious "martyrs." The AAT is reportedly linked to Al-Qaeda, and to Jaish-e-Mohammed, Lashkar-e-Toiba and Lashkar-e-Jhangvi. The AAT, which runs medical centers in Karachi, Pakistan, and Spin Boldak in Afghanistan

is accused of providing financial and logistical support as well as arranging travel for many Islamist extremists and of carrying on the activities of the previously designated Al Rashid Trust. According to the US, the AAT treated Al-Qaeda terrorists injured during fighting in Afghanistan and Pakistan in 2001. It is also accused of being involved in financing and supporting a network of international Islamist terrorist groups and bin Laden's followers in Afghanistan, raising money for Islamist extremists trying to infiltrate Iraq and maintaining links with an individual believed to have been involved in the abduction and murder of Wall Street Journal reporter Daniel Pearl. The AAT, which runs medical centers in Karachi, Pakistan, and Spin Boldak in Afghanistan, has offices in Bawalnagar, Gilgit, Mirpur Khas, Islamabad and other Pakistani cities. During a custodial interview in early 2003, according to the US Treasury Department, a senior Al-Qaeda detainee related that the Al Akhtar Trust and Al-Rashid Trust were the primary relief agencies that Al-Qaeda used to move supplies into Kandahar in Afghanistan. In 2002, the Al-Rashid Trust and Al Akhtar Trust decided to start a drive to collect donations from the business/industrial circles of Pakistan. Mullah Izzatullah, an Al-Qaeda official living in Chaman, Pakistan, was associated with both Al-Rashid Trust and Al Akhtar Trust. Al-Rashid Trust was designated by the U.S. on September 23, 2001 and by the United Nations (UN) 1267 Sanctions Committee on October 6, 2001. The U.S. Government has indicated that, as of mid-March 2002, Al Akhtar Trust was conducting all activities of the former Al-Rashid Trust.

According to the US Treasury Department, during a custodial interview in mid-April 2003, a senior Al-Qaeda detainee stated that the Al-Rashid Trust and Al Akhtar Trust provided donations to Al-Qaeda. While Al Qaeda was based in Kandahar, Afghanistan, these organisations provided donations in the form of blankets and clothing to Al Qaeda cadres. When Al-Qaeda operatives fled from Kandahar in late 2001, these organisations provided the families of Al-Qaeda operatives with financial assistance.

Country: Pakistan, Afghanistan

Key date: 2003 (Designated as a terrorist financier by US in 2003)

Sanabal Charitable Committee

The Sanabal Charitable Committee also known as the Sanabel Relief Agency Limited (SRA) was a charity operating in the UK which raised money for the Libyan Islamic Fighting Group, which was suspected of connections with Al-Qaeda. Sanabal was banned worldwide, and its assets frozen in 2006 by the UN. The SRA was formed in 1999 and had an office under the Taliban regime in Afghanistan.

Country: UK, Libya

Key date: 2006

WMD Proliferation Financiers/Sanctions

Ummah Tameer-e-Nau

Ummah Tameer e-Nau (UTN), also known as Reconstruction of the Muslim Ummah, UTN, Foundation for Construction, Nation Building, Reconstruction Foundation was a right-wing militant organisation founded in 2000 and founded by Pakistani nuclear scientists with close ties to bin Laden and the Taliban in neighboring Afghanistan.

UTN provided bin Laden and the Taliban with information about chemical, biological and nuclear weapons. UTN's members included prominent ex Pakistani scientists, retired military officers, and industrialists.

The stated purpose of UTN was to rebuild Afghanistan's infrastructure and raise money to develop the Taliban-held areas of Afghanistan. UTN reportedly had the personal support of Mullah Omar and close ties to the Taliban regime.

The UN declared Ummah Tameer-e-Nau a terrorist group after a search of the group's offices in the Afghan capital, Kabul, in 2001, unearthed documents referencing plans to kidnap a U.S. diplomat and outlining basic physics related to nuclear weapons. Documents also showed that there was a plan to mine Uranium inside Afghanistan.

Country: Afghanistan

Key date: 2001 (UN designated as a terrorist group)

Special Focus 29 Abdulrahman Alamoudi



Born in 1952 in Asmara, Ethiopia, in what is now Eritrea, Alamoudi earned a bachelor's degree in pharmacy from Cairo University and then moved to the US in 1979. Alamoudi earned a master's in business administration in 1988 from Southeastern

University in Washington and was the founder in 1990 of the American Muslim Council and American Muslim Foundation. The AMC has been described as a de facto front of the Muslim Brotherhood.

Throughout the 1990's Alamoudi showed his credentials as an outspoken Islamist assailing the US government's case against Mohammed Salameh who was arrested ten days after the first World Trade Centre bombings in

February: "All their [law enforcement] facts are – they are flimsy. We don't think that any of those facts that they have against him, or the fact that they searched his home and they found a few wires here or there – are not enough." Salameh was convicted in the bombing plot and is currently serving a life sentence in prison.

Later Alamoudi complained that the judge picked on the 1993 World Trade Centre bombers because of their religion: "I believe that the judge went out of his way to punish the defendants harshly and with vengeance, and to a large extent, because they were Muslim." later he began a public defence of Hamas: "Hamas is not a terrorist group ... I have followed the good work of Hamas...they have a wing that is a violent wing. They had to resort to some kind of violence." He later continued his Hamas defence, arguing that "Hamas is not a terrorist organisation. The issue for us (the American Muslim Council) is to be conscious of where to give our money, but not to be dictated to where we send our money."

On the positive side Alamoudi created the American Muslim Armed Forces and Veterans Affairs Council (AMAFVAC). Its purpose: to "certify Muslim chaplains hired by the US military."

In December 1993, Alamoudi attended the swearing-in ceremony of Army Capt. Abdul Rasheed Muhammad (formerly Myron Maxwell), the first Muslim chaplain in the US military, and pinned the crescent moon badge on the captain's uniform. "The American Muslim Council chose and endorsed Muhammad." The US Department of Defence certified AMAFVAC as one of two organisations to vet and endorse Muslim chaplains and in 1995 Alamoudi carried out a tour of naval installations in Florida to assess the needs of Muslims in the US Navy.

In 1996, Alamoudi spoke out in response to the arrest at New York's JFK Airport of his admitted friend, Hamas political bureau leader Mousa Abu Marzook. Months after the arrest, Alamoudi blamed Hamas suicide bombings of Israeli citizens on Marzook's detention: "If he was there things would not have gone in this bad way. He is known to be a moderate and there is no doubt these events would not have happened if he was still in the picture." He continued to defend Marzook: "Yes, I am honored to be a member of the committee that is defending Musa Abu Marzook in America. This is a mark of distinction on my chest ... I have known Musa Abu Marzook before and I really consider him to be from among the best people in the Islamic movement, Hamas – in the Palestinian movement in general – and I work together with him." In 2000

Alamoudi publicly embraced not only Hamas but Hezbollah.

At a videotaped protest in front of the White House, Alamoudi shouted, "Anybody who is a supporter of Hamas here? Hear that Bill Clinton. We are all supporters of Hamas. I wish they added that I am also a supporter of Hezbollah. Anybody who supports Hezbollah here?"

Alamoudi described a two-track political approach, advocating prayer for the destruction of the US, but counseled that while working within the US, his allies should try to change policy: "I think if we are outside this country, we can say oh, Allah, destroy America, but once we are here, our mission in this country is to change it. In 2001 Alamoudi attended a conference in Beirut with leaders of terrorist organisations, including Al-Qaeda.

In 2002, Federal agents raided Alamoudi's American Muslim Foundation during Operation Green Quest, as well as several other organisations which Alamoudi had led, staffed, or otherwise been affiliated, though the organisations were not closed down. Alamoudi then modified his tone on Hamas: Writing in the Orlando Sentinel in 2002, Alamoudi explained, "Hamas may be on the State Department's list of terrorist organisations, and may deserve that designation for some of its actions – such as unconscionable bombings of civilians – but this is not the 'Hamas' I support. What I support is the legal military defense of Palestine, and the political and humanitarian work of Hamas to provide representation to the occupied territories as well as medical, educational and other desperately needed social services to the Palestinian people."

Somehow despite all the above public statements, the Pentagon found fit for Alamoudi to start and effectively run the Muslim military chaplains programme, the State Department saw Alamoudi as an appealing representative of the US in its public diplomacy activities, making him a "goodwill ambassador" to Jordan, Kuwait, Lebanon, Oman, Pakistan, Syria, the United Arab Emirates, Yemen and elsewhere, as part of the USINFO programme.

The FBI announced that Director Robert Mueller would address the AMC's second annual national lobbying conference and the FBI called the AMC "the most mainstream Muslim group in the US." Even President Bush stood side by side with Alamoudi at a prayer breakfast on 14 September 2001.

In 2003 however the wheels started to come off for

Alamoudi and for AMC and its affiliates. Alamoudi was arrested by US federal agents as he returned from a trip to Libya, Syria and other Arab countries, via the UK. Alamoudi's first contact with the Libyans came in 1997. That was when he approached the country's Ambassador to the UN asking for help in financing the struggling American Muslim Foundation and in exchange offered help to try to unfreeze Libyan assets that the US government had frozen as part of its sanctions. Libya was still on US sanction lists in 2003 though and would only come off a year later. US citizens were not allowed to visit Libya or conduct many financial transactions with or connected to Libya. The arrest would lead to Alamoudi's imprisonment and the closure of his organisations.

The arrest would also blow open a secret plot by Libya's former President Gaddafi to assassinate the de facto Saudi Ruler Crown Prince Abdullah and Alamoudi bizarrely was at its centre. Gaddafi and Abdullah were attending a March 2003 meeting of the Arab League in Sharm el Sheikh, Egypt. Gaddafi severely criticised the Prince on live TV in open session for allowing US troops to remain on Saudi and Arab soil. Abdullah angrily replied shaking his right fist, "Your lies precede you, while the grave is ahead of you."

It was following this exchange that Gaddafi decided the Saudi leader should meet his own grave first. Twelve days after the Sharm el Sheikh confrontation, Alamoudi travelled to Libya. Alamoudi met regularly with Libyan officials and during one Tripoli visit Alamoudi met privately with Gaddafi himself. That's when Alamoudi learned that the Libyans were plotting to assassinate Prince Abdullah. Gaddafi told Alamoudi to tell his contacts among Saudi dissidents to arrange the killing of the Saudi Prince. Funding would be supplied by the Libyans. Funding generally in the form of cash began to flow and from May to June 2003, Libyan agents gave Alamoudi US\$250,000 as he continued his trips to Libya.

The plot started to unravel in August 2003, when Alamoudi received another "large quantity of cash" from the Libyans, some of which he delivered to Saudi dissidents. Then on the morning of 13 August 2003, someone speaking Arabic in a Libyan accent called Alamoudi's room at the Hilton London Metropole hotel in London, informing Alamoudi he had "something" for him. The individual arrived at his door, handed Alamoudi a small "Samsonite-style briefcase" filled with cash and left.

He put the money into his own carry-on baggage and, three days later, left the briefcase in the room

and headed to London's Heathrow airport to catch a flight to Damascus, Syria. During a routine baggage screening, UK customs officers found US\$336,900 in 34 bundles of sequentially numbered US\$100 bills. UK agents seized the money and detained and questioned Alamoudi. UK police though released him not realising the full significance of the findings.

Alamoudi then continued his travel to the Middle East. Later, a further US\$69,400 (£37,100) was seized from a property in Colindale, north London. Police said Alamoudi had left this cash with an unsuspecting friend who had no idea of its possible purpose.

UK agents informed their US counterparts of what they had found including details from his electronic address book. The next month, in September 2003, Alamoudi met again with Gaddafi telling him he'd arranged things in Saudi Arabia including with those prepared to kill Prince Abdullah. Libya then gave him US\$500,000 to pay the Saudi dissidents. Alamoudi kept US\$230,000 as a commission, which he handed off to a third party on his return to the US in London.

On 28 September 2003, Alamoudi arrived back in the US at Washington Dulles International Airport and falsely omitted from his customs form that he'd been in Libya. US agents then arrested him.

On 15 October 2004, Alamoudi pleaded guilty and was sentenced to 23 years in prison for violating economic sanctions against Libya when he accepted and transported the US\$340,000, making false statements in his application for citizenship and a tax offense for actions that included not reporting his overseas bank accounts. In the course of negotiating a plea with prosecutors, Alamoudi disclosed the Libyan assassination plot.³⁹

**Penalty: sentenced in US to 23 years in prison
Actions: American muslim leader supporting Hamas and involved in Libyan assassination plot against Saudi Arabia's crown prince.**

**Country: US, Libya, Saudi Arabia
Key date: 2003 (arrested by US following trip to Libya)**

Special Focus 30 Abdul Qadeer Khan



Pakistan's atomic weapons research programme started on 20 January 1972, when Zulfikar Ali Bhutto, the then Chief Martial Law Administrator, chaired a secret meeting of academic scientists just two years before Indian Premier Indira Gandhi

gave verbal authorisation to Indian scientists to conduct a test of a device that they had built. This was only three years after Pakistan's humiliating defeat in the 1971 Indo-Pak Winter war which had put Pakistan's existence in great danger.

During this time, Dr Abdul Qadeer Khan was working in a weapons grade centrifuge production facility in the Netherlands as senior scientist. As he learned the news, Dr Abdul Qadeer Khan went to the Pakistan Embassy in Amsterdam and approached Pakistan government officials where he offered to help and after an investigation he was accepted into Pakistan's nuclear deterrence programme.

In December 1974, Abdul Qadeer Khan met with Zulfikar Bhutto, as well as other senior advisers. During the meeting, Dr Abdul Qadeer Khan explained the importance to focus on a Uranium-based device, whereas others were convinced of a continuation of the current plutonium focus. Bhutto eventually saw the advantage of mounting a parallel effort.

It was the the uranium stream under AQ Khan that ultimately led to the first successful detonation of Pakistan's first nuclear devices on 28 May 1998, under the codename Chagai-I. Khan stated that eye-witnessing the nuclear tests, and the emergence of Pakistan as a nuclear power, was the happiest, finest, and glorified day of his life.

Abdul Qadeer Khan then established an administrative proliferation network with Friedrich Tinner and Peter Finke, in Europe through Dubai to smuggle nuclear technology establishing companies to transfer technology to Pakistan, Libya, and Iran. However, the cover was blown by British MI-6, and Finke, along with an unnamed Pakistan Intelligence (ISI) officer.

In 2003, Libya gave up nuclear weapons-related material including the centrifuges that were acquired from AQ Khan's nuclear "black market".

Pakistan is one of few countries to have diplomatic relations with North Korea, first established during the Zulfikar Ali Bhutto's regime, a socialist democratic regime in Pakistan. In 1990, it was reported that the highly sensitive centrifuge technology was being exported to North Korea in exchange for missile technologies. Khan, along with Benazir Bhutto, paid a state visit to North Korea and downloaded secret information on uranium enrichment to give to North Korea in exchange for information on developing ballistic missiles. Khan again paid a visit to North Korea with a senior army general to buy shoulder-launched missiles.

As early as 1989, Dr. Khan had offered to sell sensitive designs of centrifuge technology to Iran. Following the revelation, the Iranian government came under intense pressure from the US and the EU to fully disclose its nuclear programme. In October 2003, Iran finally agreed to accept tougher inspections from the IAEA at that time. The IAEA reported that Iran had established a large uranium enrichment facility using gas centrifuges based on designs, which had been obtained "from a foreign intermediary in 1989". The intermediary was not named but many diplomats and analysts pointed to Khan, who was said to have visited Iran in 1989. The Iranians turned over the names of their suppliers and the international inspectors quickly identified the Iranian gas centrifuges as Pak-1's, the model that Khan developed in the early 1980s.

In May 1998, the Newsweek magazine alleged that Khan had sent designs of centrifuges to Iraq, an allegation that he denied. UN arms inspectors apparently discovered documents discussing Khan's purported offer in Iraq. Iraqi officials said the documents were authentic but that they had not agreed to work with Khan, fearing a sting operation. During this time, Iraq and Pakistan had strained relations, and Iraq feared that an ISI sting operation might take place. During this time, Pakistan, through ISI, passed solid evidence to Mossad, whose [Pakistan] scientists had helped in building the nuclear programme in Libya. Also, Iraq had received a large amount of chemical stockpile from Dr Carlos Cardoen, another weapons scientist and metallurgical engineer.

In 2003, the US and IAEA successfully dismantled the Libyan nuclear programme and convinced Libya to give up its nuclear weapons-related material, including the centrifuges that were acquired from Khan's nuclear

"black market". The Libyans also turned over the names of their suppliers and A.Q. Khan was one of them.

The Bush administration investigated the centrifuge's nuclear proliferation in 2001 and 2002, focusing on Khan's personal role. In December 2002 it renewed its allegation that an unidentified agent, supposedly acting on Khan's behalf, had offered centrifuge expertise to Iraq in the mid-1990s. Khan strongly denied this allegation and the Pakistan Government declared the evidence to be "fraudulent". The US had responded by imposing sanctions in the 1990s. However, after Pakistan's contribution against terrorism and as a key ally of the US in the War on Terror, the US had removed the ban on technological cooperation between the US and Pakistan.

By the time the evidence against Khan had surfaced, Khan had become widely known in the country and held the most prestigious science role, the Science Adviser to the President.

On 31 January 2004, Khan was dismissed from his post and the Pakistan Government launched a full-fledged investigation into Khan to ostensibly "allow a fair investigation" of the allegations. Although he was not arrested, Khan was summoned for a "debriefing". In December 2003, Libya announced that it had agreed to abandon its undisclosed nuclear programme. Libyan government officials were quoted as saying that Libya had bought nuclear components from various black market dealers, including Pakistan's. US officials who visited the Libyan uranium enrichment plants reported that the gas centrifuges used there were very similar to the Iranian machines. The IAEA officials also visited the Libyan nuclear plant where they found models of Pak-1. Interpol arrested three Swiss nuclear scientists who were Khan's close associates.

The Pakistan government's blanket denials became untenable as evidence mounted of illicit nuclear weapons technology transfers. In early February 2004, the Government of Pakistan reported that Khan had signed a confession indicating that he had provided Iran, Libya, and North Korea with designs and centrifuge technology to aid in nuclear weapons programmes, and said that the government had not been complicit in the proliferation activities.

The Pakistan Government officials who made the announcement said that Khan had admitted to transferring centrifuge technology and information to Iran between 1989 and 1991, to North Korea and Libya between 1991 and 1997 (US officials at the time maintained that transfers had continued with Libya

until 2003), and additional technology to North Korea up until 2000. On 4 February 2004, Khan appeared on State controlled Pakistan Television (PTV) and confessed to running a proliferation ring where his confession was on-air by Pakistan's state and private television stations all over the country.

On 5 February 2004, the day after Khan's televised confession, President Musharraf pardoned him as he feared an extreme reaction would otherwise be the result. However, Musharraf wanted to avoid international pressure, particularly from the US. Therefore, Khan remained under continuous house arrest.

Following his confession, Khan became a major international symbol of proliferation. In February 2005, he was featured on the front cover of Time magazine as the "Merchant of Menace", labeled "the world's most dangerous nuclear trafficker," and in November 2005, the Atlantic Monthly ran "The Wrath of Khan", featuring a picture of a mushroom cloud behind Khan's head on the cover.

Still, Abdul Qadeer Khan remained extremely popular in Pakistan and was seen as a national hero of Pakistan. Science in Pakistan served as Pakistan's extreme national pride, and Khan's long association with science bought Khan a tremendous popularity. Khan's downfall affected the military regime of General Pervez Musharraf, as he was called the "Pro-American Leader". People in Pakistan openly blamed the US for Khan's house arrest. Journalists and the mainstream media came to support Khan and expressed their sympathies for him.

In May 2006, the US House of Representatives Sub-committee on International Terrorism and Non-Proliferation held a hearing titled, "The A.Q. Khan Network: Case Closed?" Legislators and experts demanded that Pakistan turn Khan over to the US and further Pakistan efforts to curb proliferation. When the news reached Pakistan, Chairman of Senate Secretariat M.M. Suomrow called a meeting to discuss the US demands. In June 2006, a Pakistan Senate sub-committee issued a unanimous resolution criticising the US Committee, stating that Pakistan would not turn Khan over to the US authorities at any given cost. In February 2009, two senior government officials announced that restrictions on Khan had been removed, allowing him to meet friends and relatives either at his home or elsewhere in Pakistan. The officials said that a security detail continued to observe his movements.

Penalty: house arrest and pardoned by Pakistan Govt
Action: clear proliferation to Iran, Libya and North

Korea

Country: Pakistan, Iran, Libya, North Korea
Key date: 2004 (confession on nuclear proliferation)

Karl Lee

Karl Lee - Li Fang Wei (aka Karl Lee), a Chinese citizen, and his company were charged with sanctions violations in supplying Iran with goods needed for its nuclear and WMD development. The Manhattan District Attorney's Office, working closely with OFAC, charged Lee with misuse of US banks and the proliferation of illicit missile and nuclear technology to Iran.

The Chinese company, known as LIMMT (aka Dalian Sunny Industries), was a major supplier of banned weapons material to the Iranian military. It sold high strength metals and sophisticated military materials, many of which were banned exports to Iran under international agreements, to subsidiary agencies of the Iranian Defence Industries Organisation (DIO).

In June 2006, OFAC designated LIMMT for its support of and role in the proliferation of WMD to Iran. The indictment charged that during the period from November 2006 through September 2008, LIMMT sent and received dozens of illegal payments through US banks by using aliases and shell companies. In all of LIMMT's transactions, the wire payments were sent to and from a limited number of Chinese banks that handled the accounts of LIMMT's front companies.

The investigation revealed that after OFAC designated LIMMT, LIMMT used aliases to continue sending banned missile, nuclear and dual use materials to subsidiary organisations of the DIO. The investigation identified subsidiary organisations set up by the DIO to procure and produce high-tech weapons systems, including: Amin Industrial Group, Khorasan Metallurgy Industries, Shahid Sayyade Shirazi Industries, and Yazd Metallurgy Industries. Some of the materials shipped from LIMMT to the DIO included specialized aluminum alloy used in long range missile production, graphite cylinders used for banned electrical discharge machines, tungsten-copper plates, tungsten-copper alloy hollow cylinders, metal powder, steel rods, tungsten metal powder 24,500 kilograms of maraging steel rods, furnace electrodes, and high carbon ferro-manganese. In addition, LIMMT and the DIO engaged in negotiations to have LIMMT send the DIO 400 Gyroscopes, 600 Accelerometers, and 100 pieces of Tantalum. Gyroscopes and Accelerometers are crucial technology for Iran's development of long range missiles. In 2011, the US State Department designated Li Wang Fei and LIMMT for more sanctions under the Iran, North Korea, and Syria Nonproliferation Act.⁴⁰

Country: US, China, Iran

Key date: 2009 (charged with US sanctions violations)

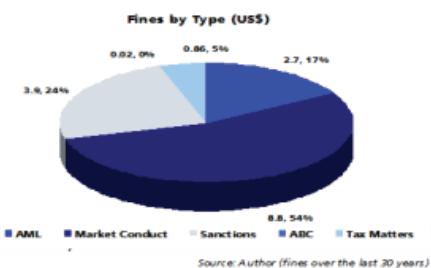
Section 8 - Enforcement Cases

Introduction,,	671
Chronology of FI Major Enforcement Cases over the last 25 years,	673
Enforcement Cases, 675	
Nugan Hand Bank, 675	
Banco Ambrosiano, 675	
Special Focus 1 - Drexel Burnham Lambert, 676	
Special Focus 2 - BCCI, 676	
Special Focus 3 - Salomon Brothers, 678	
Barings Bank, 679	
Daiwa Securities, 679	
Deutsche Morgan Grenfell, 680	
NatWest Markets, 680	
Sumitomo Corporation, 680	
Broadway National Bank, 681	
Special Focus 4 - Global Analyst Research Settlement, 681	
Special Focus 5 - Mutual Fund Scandal, 684	
GLG Partners, 686	
Citigroup Japan, 686	
Citigroup UK, 686	
AmSouth, 687	
Special Focus 6 - Riggs Bank, 687	
Oppenheimer & Company, 690	
Special Focus 7 - UBS, 690	
ABN Amro Bank, 691	
City National Bank, 691	
Banco de Chile, New York & Miami Branches, 691	
Pacific National Bank (Banco del Pacifico), 692	
New York Stock Exchange, 692	
Arab Bank, 692	
Special Focus 8 - Banco Delta Asia, 693	
Special Focus 9 - Bank of New York, 694	
Beach Bank, Miami, 695	
The Foster Bank, Chicago, 696	
Israel Discount Bank of New York, 696	
Liberty Bank of New York, 696	
BankAtlantic, 697	
Special Focus 10 - American Express Bank International, 697	
Union Bank of California, 698	
Bank of America, 699	
International Bank of Miami, 700	
Israel Discount Bank, 700	
Mizrahi Tefahot Bank, 700	
E*Trade, 701	
United Bank for Africa, 701	
Sigue Corporation, 702	
The Bank of Tokyo-Mitsubishi UFJ, 702	
Special Focus 11 - Winterflood, 703	
Société Générale, 703	
Special Focus 12 - Aon Limited, 703	
Dohu Bank, 703	
E*Trade, 704	
Special Focus 13 - Credit Suisse, 704	
Special Focus 14 - Lloyds Banking Group, 705	
Special Focus 15 - Stanford Bank, 706	
Special Focus 16 - UBS, 708	
ANZ, 708	
Amaranth Advisors LLC, 709	
Special Focus 17 - Royal Bank of Scotland (former ABN Amro Bank),, 709	
Special Focus 18 - Wachovia Bank, 711	
Deutsche Bank, 713	
Pamrapo Savings Bank, 713	
Special Focus 20 - Goldman Sachs & GS International, 714	
Trillium Capital, 714	
Royal Bank of Scotland, 715	
Special Focus 21 - Merrill Lynch, 715	
Ocean Bank, 715	
Pacific National Bank, 716	
Zions First National Bank, 716	
Mizrahi Tefahot Bank, 716	
JP Morgan Chase Bank, 717	
Deutsche Securities Korea, 717	
Lebanese Commercial Bank, 717	
Turkish Bank (UK), 718	
Mizrahi-Tefahot Bank, 718	
Coutts & Company, 718	
Habib Bank, 719	
Special Focus 22 - HSBC, 719	
UBS, 722	
Wegelin & Co, 722	
Special Focus 23 - ING Bank, 723	
Special Focus 24 - Standard Chartered, 724	
First Bank of Delaware, 724	
Allianz, 724	
Special Focus 25 - Libor Bid Rigging Scandal, 725	
National Bank Abu Dhabi, 728	
MoneyGram, 728	
SAC Capital, 729	
EFG Private Bank, 730	
UBS France, 730	
HSBC Argentina, 731	
HSBC Mexico SA, 731	
Bank of Tokyo Mitsubishi-UFJ, 731	
Barclays, 731	
Nordea AB, 732	
Panther Energy Trading, 732	
Oppenheimer & Co Inc, 733	
American Express, 733	
Guranty Trust Bank, 733	
JP Morgan Chase/JP Morgan Chase, 734/735	
Saddle River Valley Bank, 735	
TCF National Bank, 735	
TD Bank, 735	
Indian Banks, 736	
Swiss Bank Fines, 736	
Royal Bank of Scotland, 736	
JLT Speciality, 737	
Outlook Cases /2014 and beyond	

Introduction

You could certainly be forgiven for thinking that there may be a real problem in Bank Compliance with Anti-Money Laundering Laws and Regulations, based on the regular announcement of fines and penalties, particularly in recent times. Before so concluding however, a few arguments in defense of financial institutions and some observations that deserve consideration.

Whilst the number of enforcement cases has increased over the last 25 years, the increase in the number of cases itself is not that dramatic, when this is placed in the context of the size of the entire financial industry, though the penalties and the consequences certainly are with those predominantly but not exclusively being levied by Governmental Agencies in the US and to a lesser extent the UK.



Fines for sanctions breaches hit a recent record with the fines in 2012 of US\$667mio against Standard Chartered and for money laundering breaches which also included sanctions breaches of US\$1.96bio for HSBC and in 2013, against the Hedge Fund SAC Capital for US\$1.8bio for insider dealing. This following other notable fines or settlements for allegations of Fraud, against Goldman Sachs in 2010 of US\$591.5mio against UBS in 2009 for aiding tax evasion paying US\$780mio aggregated fines for conflicts in issuing US research (2003 - US\$1.4bio), US market timing and late trading (2003 - US\$3bio+) and ongoing Libor bid rigging (2012 onwards - US\$2.5bio so far).

This trend of increasing penalties can also be seen outside the Banking world, for example, GlaxoSmithKline fined US\$3bio for corrupt actions and BP for damage to the environment, currently incurring fines of US\$4.5bio (on top of costs in aggregate US\$42-65bio). Still whilst these figures for fines are staggering, large fines, at least in the US, (e.g. those in the 1980s and 1990s) have

been seen before, for example: in 1989 Drexel Burnham Lambert forfeited US\$650mio; in 1991 BCCI US\$560mio; Salomon Bros US\$290mio; and in 1996 Daiwa US\$340mio.

Whilst recognising there have been individual failings, it is of most concern, that some of the best known and most respected Financial Institutions have been fined for material weaknesses and in some cases employees wilful acts.

Top FI Penalties (>US\$100mio)		US\$
Libor Bid Rigging	2012	6bio+
Market Timing/Late Trading	2000	3bio+
HSBC (AML US Sanctions)	2012	1.98bio
SAC Capital (ID)	2013	1.8bio
US Research Settlement	2003	1.4bio
JP Morgan (Mkts)	2013	1.020bio
UBS (Aiding Tax Evasion)	2007	780mio
Std Chartered (US Sanctions)	2012	667mio
Drexel Burnham Lambert (Mkts)	1989	650mio
ING (US Sanctions)	2012	619mio
Goldman Sachs (Mkts)	2010	591.5mio
ABN /RBS (US Sanctions)	2010	580mio
BCCI (AML)	1991	560mio
Deutsche Bank	2010	553.6mio
Credit Suisse (US Sanctions)	2009	536mio
Barclays (Mkts)	2013	487.9mio
JP Morgan (Mkts)	2013	410mio
Lloyds (US Sanctions)	2009	350mio
Daiwa (Iguchi)	1996	340mio
Barclays Bank (US Sanctions)	2010	298mio
Salomon Brothers (Mkts)	1991	290mio
Bank of Tokyo Mitsubishi	2013	258.5mio
Wachovia (AML)	2010	160mio
Sumitomo	1998	150mio
RBS (US Sanctions)	2013	100mio
UBS (US Sanctions)	2004	100mio
Total (since 1989-2013)		23.45bio

Without condoning or commenting on individual cases the following may be important to note: Financial Institutions are large complex organisations employing many people in many cases all over the world. They seek to

control the activities of their employees and of course to avoid the regulatory, financial and reputation risks and costs associated with such failings but there is no risk free environment in which to operate.

Financial institutions also operate in an area subject to numerous laws and regulations, often complex, sometimes internationally producing conflicts, regularly being revised, with standards and expectations being raised without notice through inspections and as a result of greater insights, particularly changing risks and threat assessments and priorities relating to AML.

Financial institutions actively seek to identify weaknesses and continuously upgrade their frameworks and controls, and where weaknesses are material and fines and penalties are imposed quickly remediate the instant problems and at further substantial additional cost to themselves.

Whilst any case where a material fine or censure is applied to a financial institution is assumed to be a very serious case, there could be reasons and or mitigating circumstances that are rarely known or at least publicized.

Whilst there clearly are cases where employees within Banks have shown wilful disregard for complying with the law and or regulations there may be other cases where the actions or lack of them are more arguable and less clear of adjudication. It is almost impossible for a Financial Institution to disagree with the final conclusions of either regulators or other government agencies in any particular case.

The incentives to accept and consent to a fine and censure, versus fighting the case are substantial and almost always significantly outweigh any benefit in doing so. In consenting, the authorities in practise publicize their case, the case for the prosecution, whilst the Bank usually stays silent, not even offering any mitigating circumstances. Of course in some cases there may be none.

Financial Institutions have been rightly co-opted into the fight against money laundering, though that fight is principally a responsibility of Countries and governments, with Financial Institutions supporting. The standards that are applied to and the penalties levied for weaknesses found and incidents occurring are not proportionate, certainly no such similar action is taken towards Countries that have been found to be less than compliant with FATF recommendations, nor to Governments or governmental agencies directly responsible for combatting crime and for acting upon information and the much good work provided by Financial Institu-

tions in the form of Suspicious Activity Reports. A finding that a Bank failed to comply with AML laws or a regulations quite naturally, leads to legitimate questions about the Bank in question. However, the regulatory bar is set at such a high level and set to be raised even further, moving towards applying in effect strict requirements on all business lines, all accounts held and all transactions processed, requiring full compliance for millions of accounts and in many cases hundreds of millions of transactions. Some might say this is unrealistic. In criticizing Financial Institutions there is little consideration taken of the prior good work and contribution made by that institution, in coming to a conclusion on an individual matter.

Financial Institutions do not have limitless resources. Resources are already stretched and expertise is finite. Whilst the so called "risk based approach," is intended to provide flexibility to Financial Institutions to allocate resources sensibly to areas of greatest risk, this is meant to mean money laundering risk but instead the first priority is recognised by many as regulatory risk.

In particular, failing to attain required standards but also standards that continuously get tougher as good practice as a minimum standard gives way to best practice and regulatory risk increases. Financial institutions may be held accountable where a bank has not succeeded in preventing or detecting all criminal proceeds flowing into or passing through the organisation.

With these caveats and thoughts in mind here follows, the most important Bank enforcement cases, as understood from published and available sources.

Understanding what led to these censures, fines and penalties can only assist others in avoiding similar fates and improving money laundering prevention programmes.

Note: see Outlook Cases and Breaking News for further Enforcement Cases from Page 738 onwards.

Chronology of FI Major Enforcement Cases over last 25 years

1989

Drexel Burnham Lambert fined US\$650mio for market abuse leading also to its closure

1991

BCCI fined US\$10mio as well as forfeiting all American assets (US\$550mio) after pleading guilty to charges of criminal conspiracy through financial fraud

Salomon Brothers (now part of Citi) fined US\$290mio for submitting false bids for T bonds

1996

Daiwa fined US\$340mio arising out of the losses as a result of fraudulent trading by Toshihide Iguchi

1997

NatWest Markets fined £420,000 (US\$684,000) following losses by rogue trader Kyriacos Papouis

Deutsche Morgan Grenfell fined £3mio (US\$4.89mio) in connection with the actions of Peter Young

1998

Sumitomo fined US\$150mio for actions of rogue trader Yasua Hamanaka

2002

Broadway Nat Bank fined US\$4mio for AML failures

2003

Global US Settlement of 10 firms for conflicts of interest between Research and Inv Banking for US\$1.4bio

NY AG case against Canary Capital & Others fined US\$2-3bio+ (Market Timing/Late Trading)

GLG Partners fined £750,000 (US\$1.2mio) for market abuse

2004

Amsouth fined US\$50mio for AML weaknesses

Riggs Bank fined US\$25mio for AML weaknesses, quickly losing its independence and sold to PNC Bank

UBS fined US\$100mio for violating the terms of its FED Banknotes ECI agreement

Citi Japan ordered to shut its private banking operations in Japan due to AML weaknesses

Citi UK fined by UK FSA in connection with Dr Evil market trades £14mio (US\$19mio)

2005

Arab Bank fined US\$24mio for AML weaknesses

BoNY fined US\$38mio for AML weaknesses and paid US\$14mio for additional Russian claims

2006

Israel Discount Bank of New York was fined US\$12mio for AML weaknesses

Bank Atlantic fined US\$10mio for AML weaknesses

Foster Bank fined US\$2mio for AML weaknesses

2007

AMEX Bank Int fined US\$65mio for AML weaknesses

Bank of America fined US\$10.5mio for AML weaknesses

Union Bank of California was fined US\$21.6mio for AML weaknesses

2008

Sigur Corp, a NY based MSB, forfeited US\$15mio (satisfying US\$12mio penalty) for AML weaknesses

ETrade fined US\$1mio for AML weaknesses

United Bank of Africa fined US\$15.5mio

Soc Gen fined US\$6.3mio in connection with losses incurred by rogue trader Kerviel

2009

UBS fined US\$780mio for aiding clients evade US taxes

Doha Bank fined US\$5mio for AML weaknesses

CS fined US\$536mio for US sanctions violations

Aon Group fined £5.25mio (US\$8mio) by UK FSA for corruption control weaknesses

Lloyds fined US\$350mio for US sanctions violations

Amaranth Advisers fined US\$7.5mio in connection with losses of US\$6.6bio

Stanford Bank shut down

ANZ fined US\$5.75mio for US sanctions violations

2010

ABN Amro fined US\$580mio (US\$80mio/2005 and US\$500mio/2010) and 2 criminal charges for violating US Sanctions (latter fine paid by RBS)

Goldman Sachs pays in aggregate US\$591.5mio in connection with alleged fraudulent Abacus deals

RBS fined £5.6mio (US\$8.5mio) for sanction weaknesses

Wachovia fined US\$160mio for AML weaknesses later sold to Wells Fargo

Barclays fined US\$298mio for violating US sanctions

Pamrapo Savings Bank fine US\$6mio and pleads guilty to AML violations

Deutsche Bank fined US\$553.6mio for selling fraudulent US tax shelters

2011

JP Morgan Chase Bank fined US\$88.3mio for violations of US sanctions regulations

Merrill Lynch fined US\$10mio for market abuse and misuse of information

Pacific National Bank fined US\$7mio for AML weaknesses

Zions National Bank fined US\$8mio for AML weaknesses

Ocean Bank fined US\$10.9mio for AML weaknesses

Lebanese Commercial Bank forfeits US\$102mio to US government for Hezbollah contacts

2012

Coutts & Co (a subsidiary of RBS) fined £8.75mio (US\$13.25mio) for AML weaknesses

HSBC fined US\$1.98bio (US\$1.92bio by US Regulators/US\$41.8mio by Mexican Regulators and US\$21mio by Argentinian Regulators) for AML weaknesses and violating of US sanctions

ING fined US\$619mio for US sanctions violations

Standard Chartered fined US\$667mio for US sanctions violations

UBS fined £29.7mio (US\$47.6mio) in connection with Adeboji's rogue trading

First Bank of Delaware fined US\$15mio for AML weaknesses

Allianz fined US\$12.3mio for corruption failures

Barclays, RBS & UBS fined re Libor (ICAP and Rabo Bank 2013) in total US\$3.7bio (and by EU Commission US\$2.33bio also with SocGen, Citibank, JP Morgan and Deutsche Bank)

2013

Swiss Bank, Wegelin fined US\$58mio and ceases business after aiding US clients evade US taxes

Hedge Fund, SAC Capital agrees to pay US\$1.8bio to settle civil and criminal insider dealing charges

UBS fined US\$14mio in France for inadequate tax fraud controls

HSBC Argentina fined US\$21mio over 3 years for AML weaknesses

EFG Private Bank fined in UK £4.2mio (US\$6.4mio) for AML weaknesses

BTMU fined US\$258.5 mio for violations of US sanctions

Barclays fined US\$487.9mio for market manipulation in the energy markets

AMEX fined US\$5.2mio for US sanctions violations

Oppenheimer & Co Inc fined US\$1.42mio for Penny Stock compliance violations

Panther Energy Trading fined US\$5.8mio for market manipulation

JP Morgan fined US\$410mio for market manipulation in the energy markets

JP Morgan fined US\$920mio for lax controls over London "Whale"

RBS fined US\$100mio for US sanctions violations

JLT Specialty fined £1.8mio by UK FCA for anti-bribery weaknesses

Enforcement Cases

Nugan Hand Bank

1980 - collapsed¹

Agencies: N/A

The Nugan Hand Bank was a merchant bank created in Australia in 1973 by its two principals, Frank Nugan and Mike Hand. The bank had branches outside Australia, including the Cayman Islands, Washington DC, Manila, Hawaii, Cape Town, Hong Kong, Taiwan and the inauspicious destination of Chang Mai, the centre of the opium trade in South East Asia. Nugan was an Australian lawyer, while Hand was a former US military man. Nugan was purportedly an expert in money laundering and tax fraud while Hand was based in Hong Kong and focussed on drug trafficking and importation.

To establish a veil of legitimacy, Nugan Hand Bank cultivated connections to the US military services, with ex-military men serving in prominent positions in the Bank. It has also been alleged, although never proven, that the Bank was the bank of choice for the CIA throughout the 1970's. During this time the Chaing Mai branch was considered to be a central player in facilitating the money laundering associated with drug trafficking in South East Asia.

The Bank unravelled at the death of Nugan by a gunshot wound in 1980. Following this, Hand destroyed files and fled, supposedly to Fiji and thereafter Canada. The collapse of Nugan Hand Bank caused the State Government of New South Wales to institute a Royal Commission. The Commissions findings were that the Bank was a corrupt and criminal entity, prior to any real anti-money laundering regulation or supervisory oversight by banking regulators, the principals embarked on an unfettered series of criminal schemes and facilitated the laundering proceeds for individuals as diverse as Abe Saffron, the 'Mr Sin' of Australian criminal life throughout the 1960's and 1970's and even the now known kleptocrat, the former president of the Philippines, Ferdinand Marcos. Nugan Hand was also central in the 'bottom of the harbour' tax evasion schemes, which operated in Australia at this time. These schemes essentially involved asset stripping from companies that had tax liabilities and transferring those assets to 'phoenix' corporate entities in order to defraud tax authorities.

Banco Ambrosiano
1982 - collapsed²
Agencies: N/A

The body of Roberto Calvi, an Italian banker, was found in 1988 hanging from scaffolding beneath Blackfriars Bridge in the financial district of London. Calvi, director of Banco Ambrosiano (BA), allegedly hanged himself following the fraudulent bankruptcy of the bank. Calvi's clothing was stuffed with building bricks, and he was carrying around US\$15,000 of cash in three different currencies.

Calvi, dubbed by the press as "God's Banker" due to his close association with the Vatican, had gone missing on June 10. In 2003 RAI state television said prosecutors believed the Mafia killed Roberto Calvi because he lost their money and knew too much about their operations.

In 2005 a trial began for 5 people in the murder of Calvi. In 2007 however a jury acquitted all 5 defendants charged. Following a two year trial of executive employees at BA, on the 16th of April 1992 the Criminal Court of Milan found guilty all 33 defendants charged with causing the collapse of their financial institution.

BA famously collapsed with US\$1.3bio of un-refunded loans. Significantly a total sum of US\$1.1bio in loans was made to dummy companies in Panama, set up by the Vatican bank Instituto d'Opere Religiose (IOR). US\$200mio was also lent directly to the IOR. Chief among those executives responsible for the mismanagement and subsequent collapse of BA was Roberto Calvi, who was Chairman to Banco Ambrosiano Overseas Limited (BAOL), one of BA's foreign subsidiaries. However Calvi also established Banco Ambrosiano Andino (BAA) as a holding company. Loan agreements would be partly made in Milan, to be processed later in Luxembourg for tax reasons, a lawful transaction sequence, but one that allowed Calvi to administer his business outside the oversight of Banco Ambrosiano SpA (Italy) (BI). For instance in October 1979 IOR accepted two deposits worth US\$134.2mio in total from BA's Peruvian subsidiary, which it subsequently lent to a Panamanian company. This Panamanian company, (owned by IOR) later bought BA stock with the funds it had borrowed. In this manner Calvi effectively facilitated the buying of BA stock by IOR using BA's own funds. The covert affair was intended to prevent what Calvi would deem a hostile takeover of BA, placing stock in the friendly hands of the Vatican Bank IOR. As it was these loans played a crucial part in the bank's financial collapse, and only a day prior to his death Calvi was stripped of his position as Chairman.

Special Focus 1 Drexel Burnham Lambert

1989 - US\$650mio³

Agencies: DOJ, SEC

With the benefit of hindsight it seems that the revenue generating capability of star banker Michael Milken and his department became so large within Drexel's overall business that the fate of both became almost inexplicably intertwined. From the earliest negotiations with Giuliani the Government's insistence that any settlement had to include the removal of Milken from the firm was a huge sticking point and an unacceptable step too far for Drexel's management.

Also with the benefit of hindsight one cannot help wondering the extent to which Milken's department based as it was on the West Coast of the US formed, in effect, its own 'firm within a firm' removed from the oversight and governance processes that might apply elsewhere.

Some have noted that Drexel adopted a highly "meritocratic" and aggressive business culture. It is also perhaps noteworthy that Drexel had little ability to bring in outside capital and relied very significantly on its ability to raise money through wholesale funding including, in particular, its commercial paper programme. It seems that its inability to continue to finance itself through the wholesale markets was the final trigger which led to Drexel's filing for Chapter 11 Bankruptcy Protection.

The zeal and aggression with which the authorities pursued Milken in particular but also Drexel was astonishing and even at that time caused some disquiet amongst certain commentators and academics. For example, Milken's brother, Lowell was threatened with indictment despite having little obvious connection with the matters under investigation other than increasing the pressure on Milken to settle. Federal investigators also questioned Milken family members including his aging grandfather about their investment activities. The use of the draconian powers available under RICO was largely unprecedented. The wrongdoing to which Milken eventually agreed to plead guilty had never before and had never since been dealt with as a criminal matter.

The penalties levied on Milken were ultimately huge

and arguably out of all proportion to the crimes for which he was convicted. At trial the judge estimated that the injury for all counts to which Milken pled guilty combined together was US\$318,000. In addition to the 22 months he served in prison, Milken accepted a lifetime ban from the securities industry, agreed to pay US\$200mio in fines, and agreed to a settlement with the SEC in which he paid US\$400mio to investors who had been hurt by his actions. In a related civil lawsuit he agreed to pay US\$500mio into a fund to compensate Drexel's investors. In total Milken paid US\$1.1bio for all lawsuits related to his actions while working at Drexel. Drexel was fined US\$650mio in January 1989 prior to its continued downfall and filing for bankruptcy in February 1990.

Special Focus 2 BCCI

1991 - US\$10mio fine and forfeiture US\$550mio / forced shutdown^{4/5/6}

Agencies: DOJ, BofE

The Bank of Credit and Commerce International (BCCI) was founded in 1972 and pursued an aggressive expansion programme which saw it grow from a network of 19 branches to one of 108 branches by 1976. Its assets grew during the same period from US\$200mio to US\$1.6bio and it continued to be the subject of considerable press speculation that it suffered from a lack of adequate oversight and control which had undermined its capital stability. The Bank was split into two separate operating companies, BCCI SA (Luxembourg) and BCCI (Grand Cayman) each located in a jurisdiction where, at the time at least, banking supervision was considered to be less stringent. In addition, all the 248 managers and general managers reported to the two main directors giving them an unusual ability to direct and control operations as well as leading to a lack of clarity within the company about its overall direction and financial standing. In addition, the complex nature and number of its corporate entities and structures made it possible to evade legal restrictions on the movement of capital and goods as well as confusing auditors and confusing external investigators.

There was also considerable concern at the lending practices at BCCI which frequently involved activities in areas where banking services were less extensive and with individuals who either had close personal connections with the senior management of the bank or whose source of wealth was the result of questionable activity.

One example was the BCCI relationship with the Gokal family, a prominent family involved in the shipping industry with connections to Agha Abedi, the bank's founder, that was extensive and dated back to his employment at a previous financial institution. Rather than route these transactions through the normal commercial lending teams, Abedi handled this relationship personally often allegedly failing to complete the requisite loan documentation or securing appropriate collateral. At one point, the value of loans extended to this family was more than three times the entire capital of BCCI at that time a position that far exceeded usual regulatory guidelines.

In addition, subsequent investigations revealed that it had undertaken significant transactions with and on behalf of clients such as Saddam Hussein and Manuel Noriega. It was also alleged to have maintained accounts on behalf of the Medellin Cartel and the Abu Nidal Organisation.

Perhaps an indication that it was willing to offer accounts to anyone with funds to dispense without asking questions, the CIA allegedly held multiple accounts with the institution which were used to finance and support its clandestine operations in a number of jurisdictions according to William von Raab the former US Commissioner of Customs.

By 1998 the bank had been implicated in a scheme to launder drug related proceeds through an operation in Tampa (the so-called C-Chase case). It eventually pleaded guilty to the charges and was forced by Florida regulators to pull out of the state but the Federal regulators took no action. They were, however, keen to ensure that BCCI was unable to establish a significant banking operation within the US which resulted in the Bank taking considerable steps to disguise its involvement in the subsequent takeover of an American based institution.

Despite these obstacles BCCI, using a set of front companies and US persons, eventually acquired a total of four US financial institutions with operations in seven States. The preferred method was to make the purchases through nominees and ensuring that it had an active network of lawyers and publicity agents whose activities further dissuaded investigators from exploring its true ownership and business activities. In addition, BCCI had been using two different auditing firms to ensure that no single overview of the business was possible and this situation was further compounded by discovery of the fact that the bank had been making loans and other financial benefits to some of its auditors a practice which, at the very least, created an impression

of impropriety.

In 1988 and 1989 the Bank of England, concerned at ongoing speculation about BCCI's alleged involvement in the laundering of drug money and financing of terrorism undertook additional and limited supervisory action. Then, in the spring of 1991, the external auditors, Price Waterhouse, submitted a report to the Bank of England stating that they had uncovered evidence of poor banking practices including the provision of improper loans and indicators that fraud had been taking place. Sections of this report (known as the Sandstorm report) were subsequently leaked to the British Media and included allegations that the Abu Nidal terrorist group had maintained accounts with the bank as well as details of letters of credit valued at millions of dollars which had been used to facilitate the purchase of arms for Iraq.

At this point, BCCI had moved its headquarters to Abu Dhabi and, through a process of restructuring was attempting to regularize its affairs, a process that would have seen it rebranded as the "Oasis Bank" but regulators had already concluded that the bank's situation was so dire that the only option was to take action to shut it down.

Working in a coordinated manner, regulators in five different jurisdictions took action in July 1991 to liquidate the company entering BCCI offices around the world and shutting them down, action which immediately impacted around a million depositors. A few weeks after this action, the New York District Attorney announced that a grand jury had indicted BCCI and its two main officers on charges of fraud, money laundering and larceny following a two year investigation. It claimed jurisdiction on the basis that millions of dollars that had flowed through the bank had all passed through Manhattan.

Shortly afterwards, BCCI pleaded guilty to all charges and agreed to pay US\$10mio in fines as well as forfeiting all its American assets (US\$550mio) which were partially used to repay US investors.

The British Government also undertook an independent investigation (the Bingham enquiry) which made a number of critical comments about the actions undertaken by the Bank of England. Following its publication, thousands of creditors sued the Bank of England claiming that it had failed to oversee BCCI to a satisfactory standard although the case was later to collapse.

Special Focus 3 Salomon Brothers

1991 - US\$290mio⁷

Agencies: US DOT, CMP

Salomon Brothers was a bulge bracket, Wall Street investment bank. Founded in 1910 by three brothers (Arthur, Herbert and Percy) along with a clerk named Ben Levy, it remained a partnership until the early 1980s, when it was acquired by the commodity trading firm Phibro Corporation and then became Salomon Inc. Eventually Salomon was acquired by Travellers Group in 1998, and following the latter's merger with Citicorp that same year, Salomon became part of Citigroup. Although the Salomon name carried on as Salomon Smith Barney, which were the investment banking operations of Citigroup, the name was ultimately abandoned in October 2003 after a series of financial scandals that tarnished the bank's reputation.

The most infamous of which was the US government bond bid rigging scandal that threatened Salomon's existence in 1991. Salomon was run at the time by its then CEO the legendary John Gutfreund who had risen through the firm to become CEO in 1978.

During the 1980s, Salomon was noted for its innovation in the bond market, selling the first mortgage-backed security.

Salomon purchased home mortgages from thrifts throughout the US and packaged them into mortgage-backed securities, which it sold to local and international investors. Later, it moved away from traditional investment banking (helping companies raise funds in the capital market and negotiating mergers and acquisitions) to almost exclusively proprietary trading (the buying and selling of stocks, bonds, options, etc. for the profit of the company). Salomon largely focussed on fixed income securities and trading based on daily changes in the bond market and was led by John Gutfreund.

Gutfreund was a fabled gruff-talking, cigar-chomping bond trader. According to Liar's Poker, a 1989 best seller by Michael Lewis that described Salomon as a sort of financial Animal House, Gutfreund exhorted traders to come to work each morning "ready to bite the ass off a bear." When the traders were not executing centimillion-dollar deals, they delighted in such pranks as dumping garbage on one another's desks and replacing the contents of a male colleague's suitcase with

lingerie.

For decades, the government securities market was considered the world's safest haven for investors. Unlike stocks which had been plagued by a series of insider-trading cases during the 1980s, the US\$2.2 trillion market for US Treasury instruments was thought to be too big to rig. Regulations prohibited any one bidder from buying more than 35% of a single issue at a Treasury auction. The rule was designed to prevent price-fixing in the Treasury market. Pensions, life insurance and mutual funds depend on the price of US Treasury securities, as do taxes, interest on mortgages and the debt burden of private companies so ensuring this market is not artificially driven up or down is critical.

Salomon trader, Paul Mozer had been submitting false bids in an attempt to purchase more Treasury bonds than permitted under the 35% rule during the period between December 1990 and May 1991. In an elaborate form of hazing, Mozer had persuaded a Salomon customer to submit a bogus US\$1bio order for 30-year Treasury bonds, to shock a novice trader who received the order. As it turned out however the deal went through, and the unauthorized purchase landed on Salomon's books. This led Mozer to continue the practise and by using clients' names he was able to secretly exceed the 35% limit on control of a single issue and to artificially drive up the price of those securities.

Salomon rigged bids to exceed the 35% trading ceiling in at least three Treasury auctions during a nine month period. In December 1990 for example the firm bought 35% of a US\$8.5bio, four-year-note sale and also submitted a US\$1bio bid that was ostensibly for a customer but was really for its own account. The combined transactions gave Salomon a 46% share of the overall deal.

Complaints from investors who lost an estimated US\$50mio to US\$200mio in one May 1991 Treasury auction prompted a federal investigation. In the US\$12.26bio May auction, Salomon is believed to have gained control of 85% of the issue by bidding under customers' names.

Some investors, who took "short" positions on that issue, essentially betting the prices of the May notes would fall, lost because of the increases in prices that followed.

Whilst Salomon senior management, including Gutfreund, Strauss and Merriweather already learned of these breaches, being notified by the Company's

General Counsel, they did not act to inform the US Treasury, only doing so following the initiation of the Federal investigation. The firm announced that they had failed to report the violation "due to a lack of sufficient attention" to the matter. When eventually notified the US Treasury Department was infuriated.

The Treasury Department, in an attempt to restore confidence in the market, immediately barred Salomon from bidding at further auctions and began an investigation. There was even consideration given to bringing criminal charges against the firm. Instead the firm was fined US\$290mio, the largest fine ever levied on an investment bank at the time. CEO John Gutfreund was forced out of the company leaving in August 1991, taking a personal fine for failures to supervise of US\$100,000 and he was barred for life from serving as a chief executive of a brokerage firm.

The decision to ban Salomon from the T bill auctions was more serious however, with Salomon, one of only 40 firms designated as primary dealers in T-bonds and T-bills, this was not a problem for the US Treasury but with dealing in US government securities accounting for about 25% of Salomons business, it was a major risk to Salomon's existence.

In stepped Warren Buffet, a man who was at the time a 16% owner of Salomon's preferred stock and who had a legendary reputation for investing. He took over as interim Chairman and CEO following John Gutfreund's departure. In a series of telephone calls with Treasury Secretary Nicholas Brady, Buffet successfully lobbied for leniency. Salomon was permitted to trade, but for its own account only, not on behalf of clients. The firm thus survived. As one of his first actions as interim CEO, Buffet wrote a letter to all his managers, providing them with his home phone number in Omaha and telling them if they saw anything unethical, to give him a call. The firm rehabilitated its reputation under Buffet's leadership but was still undoubtedly weakened by the scandal. The firm was bought out by Travellers Group, under CEO, Sandy Weil which would later merge with Citigroup.

The combined investment banking operations became known as "Salomon Smith Barney" for a time but the name Salomon was eventually retired in favour of "Citigroup Global Markets."

The scandal was then documented in the 1993 book *Nightmare on Wall Street*. Two members of the Salomon Brothers' bond arbitrage team, John Meriwether and Myron Scholes, later became a founder and a consultant for Long-Term Capital Management,

a hedge fund that collapsed in 1998. The firm's top bond traders called themselves "Big Swinging Dicks," and were the inspiration for the book *The Bonfire of the Vanities*, by Tom Wolfe. Salomon Brothers' success and decline in the 1980s is documented in Michael Lewis' 1989 book, *Liar's Poker*. Lewis went through Salomon's training programme and then became a bond salesman at Salomon Brothers in London.

Barings Bank

1995 - collapsed and insolvent⁸

Agency: Monetary Authority of Singapore

On 17 January 1995 a massive earthquake shook the Japanese city of Kobe, as well as shaking one of the oldest of Britain's financial institutions, Barings Bank, which would be brought down by Rogue Trader, Nick Leeson who had bet heavily on a rise in the Japanese stock exchange. Losses eventually reached US\$1.4bio, twice the Banks available capital, leading to the insolvency of this venerable institution. For more details see the case of Nick Leeson in Part 2, Section 7, Criminal Cases, Rogue Traders.

Daiwa Securities

1996 - US\$340mio^{9/10}

Agencies: US DOJ, US FED

On 13 July 1995 Toshehide Iguchi, then Executive Vice President of Daiwa's New York Branch and head of its Securities Custody Department sent a personal letter to "Mr. Fujita," the President of Daiwa Bank Ltd, at Daiwa headquarters in Osaka, Japan. In the letter, Iguchi would confess that in trying to cover up a US\$70,000 loss made in 1983, he had caused a US\$1.1bio loss from unauthorised proprietary trading and unauthorised sales of client's holdings in US Treasury Bonds. Iguchi further stated that he believed Daiwa should "keep the secret until the bank and possibly the Japanese authorities can take appropriate measures." For more details see Part 2, Section 7, Criminal Cases above.

Whilst the losses were shocking what came next compounded the problems for Daiwa and would lead to the US authorities forcing Daiwa to close their business in the US. Daiwa management in Japan and in New York conspired to conceal the losses. Instead of reporting the fraud to the authorities as they were legally compelled to do, the management went to incredible lengths to cover up the losses. Daiwa, at Iguchi's suggestion, agreed to try to use its large capital reserves to replace the losses to clients by continuing to trade, hoping to make profits and to replace the losses. Using fraudulent documentation, making false disclosures, pretending that Iguchi was on annual leave, so that an audit had to be postponed and even

disguising the nature of his trading department, in order that it appeared as a back office function, Daiwa acted appallingly. It was only after it became apparent that the additional trading was producing continued losses and that this would be unsustainable that they instructed Iguchi to confess his crime to the US authorities. In November 1995, Federal prosecutors in NY unveiled a criminal indictment and ordered Daiwa to shut down all operating in the US within 90 days. Daiwa initially pled not-guilty but by February 1996 they changed that plea to guilty and were fined US\$340mio. In 1996 Daiwa closed down its 15 US offices, selling US\$3.3bio of assets to rival Sumitomo Bank in the process. The effect on the bank was more lasting though with a revision to a deposit taking institution and a drastic reduction of their global presence. As a result of the losses, but more importantly, Daiwa's attempt to cover them up and not to directly inform regulators, what was once a sizeable institution with a global presence had been reduced to little more than a medium sized national bank.

Deutsche Morgan Grenfell

1997: £3 mio¹¹

Agency: IMRO (UK regulator, one of the predecessor regulators prior to UK FSA)

IMRO, the Investment Management Regulatory Organisation fined DMG £2mio handing down the largest fine ever imposed under the UK Financial Services Act, for the mishandling of investors' funds by its former star manager Peter Young which was almost three times higher than the previous record. Additional costs of over £1mio were also levied to cover the investment management regulator's costs.

Phillip Thorpe, Imro chief executive, said: "The mismanagement of these funds has caused unnecessary concern to an enormous number of investors. The firm has paid dearly as a consequence of inadequate management control. This affair plainly illustrates the dangers of ignoring clear and repeated warnings." The fine came eight months after Morgan Grenfell fired Mr Young for breaking regulations by investing too much of three funds' assets in unlisted shares. Five other executives, including his supervisor, Mr Percy, were ousted for failing to monitor his dealings. Mr Young had invested in dozens of hi-tech companies, breaching the 10% limit in unlisted assets that can be held by unit trusts. He concealed the investments in part through a complicated web of holding companies based in Luxembourg. IMRO said Morgan Grenfell International Fund Management "did not organise and control its internal affairs to ensure its funds were properly managed" and said it "did not act with due skill, care and diligence when it failed to prevent the funds from making inappropriate investments".

NatWest Markets

1997: £420,000 fine^{12/13}

Agency: UK SFA (predecessor to UK FSA)

In 1997, NatWest Markets (NWM), the corporate and investment banking arm of one of the UK's largest banks, National Westminster Bank now part of the Royal Bank of Scotland Group revealed that a £50mio loss had been discovered in its interest rate options and swaptions trading books. The loss figure escalated to £90.5mio after further investigations and the trader involved was Kyriacos Papouis. The regulator imposed a penalty of £420,000 on NWM, and fined and reprimanded Papouis as well as his supervisor, Neil Dodgson for breaches of SFA principles. But the real damage was to the reputation of National Westminster Bank itself, and with confidence undermined, the Bank fell in a hostile takeover soon after.

Sumitomo Corporation

1998: US\$150 mio¹⁴

Agency: US CFTC

Sumitomo Corporation agreed to pay US\$150mio in fines and restitution, arising out of charges that its lead copper trader Yasuo Hamanaka, manipulated the copper market in 1995 and 1996. The CFTC order explained how Hamanaka, tried to drive up the price of copper, beginning in late 1993. Nearly all the buying took place on the London Metal Exchange. "During the summer of 1995 and through the fourth quarter of 1995," the commission's order said, "Sumitomo's copper trader and the U.S. copper merchant plotted and executed their scheme to push copper prices to an artificially high level and then exit the joint operation by liquidating" their large positions. "The focus of these operations ultimately was the acquisition of all of the stocks of deliverable copper in L.M.E. warehouses," it said. By 24 November 1995, according to the commission, Sumitomo owned 93% of all London Metal Exchange warehouse copper through one brokerage house, and together with the American operation had all the copper. One might think that would have left Sumitomo in a great position to force up the price. But by then the copper price was heading down. Copper for delivery in the next month was then priced at US\$1.3145 a pound, down from a peak of US\$1.461 on 13 July. In the end, Sumitomo's purchases did a fine job of running up the price. The spot price of the metal, which was low as 72 cents a pound in the fall of 1993, when the commission says Mr Hamanaka began talking about driving up the price, had more than doubled by the time it reached its peak. The rise came as Sumitomo was accumulating more and more copper. In cornering a market, one or more conspirators acquire all that is available of a given item, forcing short-sellers who had bet against the rise to pay high prices when they buy the item to cover their

short positions. But the trick is in then selling the rest of the position still at a high price. High prices tend to discourage consumption and to increase production.

Still, Sumitomo still had large positions when the conspiracy unraveled in the spring of 1996, ending with a loss of US\$2.6bio. One of the most significant aspect of the CFTC order was the way the commission asserted it had jurisdiction over the case. There was some trading in the US, and the London Metal Exchange has a warehouse in California. Either might have been a sufficient basis to establish jurisdiction. But the commission went further, asserting it had jurisdiction because the conspiracy drove up prices on the Comex in New York, where copper futures are traded. Given that commodity markets around the world reflect similar prices, the CFTC action implies that manipulation of any commodity traded in the USA country could be the subject of a CFTC action, even if no acts were committed in the US.

Broadway National Bank
2002 - US\$4mio CMP^{15/16}
Agencies: US Customs / IRS

Broadway National Bank was found guilty in Manhattan on three criminal charges for failing to file suspicious-activity reports on US\$123mio in cash deposits and failing to establish a programme to curb money laundering and fined US\$4mio.

From 1996 to 1998, the bank failed to report hundreds of bulk cash deposits totalling more than US\$46mio and thousands of transfers structured to avoid disclosure laws. Once the cash was deposited, sometimes in large duffel bags dropped off in the teller area, it was quickly wired to bank accounts abroad. US\$20mio was established in accounts maintained by members or associates of the Fares family, five of whose members have been convicted of laundering drug money. One client told bankers he was in the electronics business, deposited US\$46mio into nine accounts, sometimes in cash installments as large as US\$660,000. This client pleaded guilty to laundering money on behalf of a Colombian Drug Cartel. Bankers made no effort to visit the clients listed place of business, which was a few blocks from one branch. Had they done so, they may have noticed that it was vacant.

"This bank had become the bank of choice for criminal organisations because it didn't ask questions and didn't want to know where the money came from," said a spokesman for the Customs Service, which investigated the bank with the US IRS.

Special Focus 4 Global Analyst Research Settlement

2003 - US\$1.4bio^{17/18}

Agencies: NYAG (Spitzer), SEC

In August 1991 Tim Berners-Lee, a CERN researcher, first posted details of his creation - the "World Wide Web" - on the internet and invited the world to download his software and create their own websites. Four months later Paul Kunz, a Stanford scientist, launched the first US website. By 1993, the internet had over a million computers attached to it and according to a 1994 Time article was "growing faster than OJ Simpson's legal bills". But (and it was big 'but') the internet was run by the US government: a user had to agree to use it for "research and education" only. The idea of making money through commerce on the internet was in its infancy. After consultation, the US government formally ceased running the internet on 30 April 1995 and handed it over to private enterprise. The starting gun was fired in the race for commercial development of the internet.

Over the next 6 years, with increasing momentum, the dot-com boom gathered pace across mainly US and European markets. Despite occasional hiccups, the frenzy of activity was driven and fuelled by media hype, floods of money from venture capitalists and other investors, a benign macro-economic policy and a belief that the internet and e-commerce represented a new paradigm for commercial opportunity and success. Household names such as Amazon and Yahoo! were born and survived. Many others crashed and burned. Even the survivors traded at times on eye-watering multiples when compared with traditional valuations for companies. In late 1999 with its stock price at over US\$500 Yahoo! was valued at over US\$131bio - 2,154 times its 1999 earnings and more than Walt Disney and News Corporation combined.

After initial financing, the first real goal for many start-up companies rushing to secure a place in the promised land of e-commerce was to complete an initial public offering (IPO). In this the company would sell its shares to - hopefully enthusiastic - public investors for the first time and in the process make the company's founders and original shareholders (often venture capital firms) very wealthy. The IPO process is organised and run by investment banks, who charge a healthy fee (then in the US up to 7% of the IPO proceeds) for doing

so. Traditionally, a start up company would trade for a number of years and establish a track record of being a sound and profitable business before even considering an IPO. With the dot-com boom, all that changed. New start ups rushed to the public markets with astonishing haste. In some cases, these IPO candidates were little more than a catchy name and a business plan.

A couple of examples amongst many: in early 1996, CyberCash went public issuing 2mio shares at US\$17. In a week the shares had risen to US\$50 - even though in the 17 months between its incorporation and going public CyberCash had lost US\$10mio and had total revenues of - zero. As an S&P analyst in refusing to recommend the shares noted "the lack of any sales was a major negative in our rating." In late 1998, EarthWeb - an on-line publishing company - went public, selling 2.1mio shares. On the first day of trading its stock jumped from US\$14 to US\$48. Its founders - two brothers from Brooklyn - were worth on paper at least US\$65mio each - despite in the first half of 1998 EarthWeb managing to lose US\$5.3mio on total revenues of just US\$1.9mio.

The University of Michigan Business School even started a course entitled "From idea to IPO in 14 Weeks". One UBS compliance officer recalls attending - in all seriousness - a commitments committee (not at UBS) and discussing a start up's idea to put small web cameras on jockeys during horse races and streaming live pictures over the internet from "your horse" to gamblers for a fee. The proposal was rejected - amongst other concerns it was thought the main view would simply be of the backs of the horses' ears. In March and April 2000 the bubble finally burst and the party was over. Many internet companies' share prices fell like a stone - true to an old London Stock Exchange adage comparing shares to fireworks: "up like a rocket, down like the stick".

Many companies ultimately disappeared without a trace: either closing down or finally using up all their available cash. Investors - including many private investors - lost large sums of money. Inevitably people began to cast around for those to blame. Whilst there were many contributing factors and many cheerleaders for the dot-com boom, particular focus started to alight on the role of internet research analysts and their relationship with the Investment Banking Departments at major Wall Street firms.

Many firms had earned huge investment banking fees during the internet boom. Firms had significantly built up their internet research coverage with "star" analysts such as Henry Blodget at Merrill Lynch, Jack

Grubman at Salomon Smith Barney and Mary Meeker at Morgan Stanley to the fore. In particular, there were concerns that the traditional separation between Investment Banking and Research had been eroded and that far from offering sober and independent analysis of companies, analysts had become far too close to investment bankers and their clients.

Beginning with Merrill Lynch, Eliot Spitzer the New York Attorney General began aggressively investigating Wall Street firms for evidence of fraud and malpractice in connection with their research activities. Ultimately this investigation led to a Global Analyst Research Settlement between 10 firms and US regulators. Under this court-sanctioned settlement, the firms paid a total of over US\$1.4bio in penalties. In addition the firms agreed to fundamental reform of their research practices including structural reforms entirely separating Research and Investment Banking, greatly enhanced disclosures in research reports, the requirement to buy and offer to customers independent research and payments into an investor education fund. The separation and disclosure requirements broadly survive to this day.

Spitzer's main initial target was Merrill Lynch and their Head of Internet Research, Henry Blodget. During the course of his investigation Spitzer found evidence of widespread bias and distortion in Merrill's research ratings. Merrill had a five category stock rating system (buy, accumulate, neutral, reduce, sell). Between Spring 1999 and Autumn 2001 Merrill never published a single reduce or sell rating on any stock covered by the Internet group. He also found that at the same time that analysts had positive published ratings on a company their Internet analysts were privately disparaging that very same company. Emails showed stocks on which analysts had buy or accumulate ratings being privately described by analysts as a "piece of junk" (InfoSpace), a "piece of shit" (24/7 Media) or "such a piece of crap" (Excite@Home). Emails also showed that the Internet Research Group was not independent to the Investment Banking Department. Within weeks of joining Merrill, Blodget as Head of the Internet Research Group sent around a memo entitled "Managing the banking calendar for internet research". The memo unapologetically described his expectation that at least half his and his team's time would be allocated to investment banking matters and described Blodget's work schedule for one week as being divided "85% banking, 15% research". Indeed Merrill's research management itself acknowledged at one point that "we are off base on how we rate stocks and how much we bend backwards to accommodate banking". Spitzer's investigation also found that in some cases proposed ratings were discussed and agreed

with investment bankers and indeed on occasion the covered company itself in breach of internal Merrill policy. Research analysts' remuneration was also at least partly determined by investment bankers. In Autumn 2000, the Co-head of Global Equity Research informed all equity analysts "we are once again surveying your contributions to investment banking please provide complete details on your involvement in the transaction paying particular attention to the degree that your research cover played a role in origination, execution and follow up. Please note your involvement in advisory work on mergers or acquisitions especially where your coverage played a role in securing the assignment". In response, Blodget confirmed his group had been involved in over 52 completed or potential transactions which had earned US\$115mio for Merrill. Identified services his analysts provided to investment banking included pitching to the client, marketing the offering and initiation and follow on research coverage. In publishing a recommendation on GoTo.com in January 2001 an institutional investor asked Blodget what was interesting about the company except banking fees. Blodget replied "nothin". Of course such intertwining of Research and investment banking led to tensions and conflicts and in late 2000, for example, Blodget threatened to start to rate stocks honestly, no matter what the investment banking consequences were. His ultimatum was prompted by a long time private client broker who felt his clients were being burned by late downgrades of covered stocks and an email from Research management about downgrades. Blodget wrote an email threatening they would "just start calling the stocks like we see them no matter what the ancillary business consequences are". To conclude the investigations of Merrill Lynch's conduct - which was characterised by Spitzer as a "shocking betrayal of trust" - the firm settled with a penalty of US\$100mio. The star analyst Blodget was censured, permanently barred from the industry and fined US\$2mio.

Jack B Grubman was the star technology analyst at Salomon Smith Barney (SSB) - then part of Citigroup - through the height of the internet and technology boom. Rated 1# on the Institutional Investor All America Research team his views on companies were highly influential. His coverage universe included a host of technology companies including AT&T, Worldcom and Global Crossing. As a 2002 Money Magazine article (with the catchy title 'Is Jack Grubman the worst analyst ever?') observed "he was at the heart of the telecom debacle (and) at about US\$20mio a year... Wall Street's highest-paid analyst ever". Inevitably Grubman, as with Blodget, was enmired in the same conflict of interest issues. As a 2002 FT article had it, "to critics he embodied the untenable conflicts of

interest that characterised the boom years. He tried to bridge the traditional gulf between investment banking and equity analysis - between being a confidential adviser to corporate chieftains and an independent commentator on their companies". Grubman of course may have rationalised things differently. "What used to be a conflict is now a synergy" he told Business Week in 2000 "Objective? The other word for it is uninformed".

In the bursting of the bubble two companies that both SSB and Grubman were particularly close to - WorldCom and Global Crossing - went bankrupt. SSB, Citigroup and Grubman were part of Spitzer's investigations and the Global Analyst Research Settlement. In addition they were deluged with litigation and class action lawsuits filed on behalf of aggrieved investors who had lost huge amounts of money - notably in WorldCom and Global Crossing. Whilst these were generally settled out of court, the various actions and investigations unearthed the usual (and unusual). Reaching to the very top of Citigroup it was suggested Grubman had produced positive research on AT&T to curry favour with the company for Citigroup's bankers - Sandy Weill (Citigroup's Chairman) was forced to admit that he had personally suggested Grubman "take another look" in his research at AT&T despite earlier maintaining he never interfered in research. Grubman also confided to a friend that he changed his research outlook on AT&T as a quid pro quo for Weill helping to get Grubman's twin kids into the 92nd Street Y - a prestigious local children's school. As Weill clarified "I tried to help Mr Grubman because he was an important employee who asked for my help". Around the same time Citigroup Foundation made a US\$1mio donation to the 92nd Street Y.

Retrieved emails also found considerable evidence of the inevitable conflict of interest issues and institutional and management failure to deal with them. Ahead of a dinner with the Head of Research and some senior bankers Grubman wrote, "See you at dinner. If (a banker) starts up I will lace into him... most of our banking clients are going to zero and you know I wanted to downgrade them months ago but got huge pushback from banking". As with Blodget also found were discrepancies between published ratings on companies and the analysts private views. For example in early 2001 Grubman published a Buy recommendation on Focal Communications (a broadband telecoms provider) despite privately believing the company was "a pig". When he heard Focal had complained that his research was not positive enough Grubman wrote to two SSB bankers "I hear company complained about our note. I did too. I screamed at (the analyst) for saying 'reiterate buy'. If I hear one more

fucking peep out of them we will put the proper rating (i.e. underperform not even neutral) on this stock which every single smart buysider feels is going to zero".

There were also inevitable tensions and conflicts with SSB's large retail brokerage operation. In both 2000 and 2001, Grubman was ranked dead last of all SSB analysts by SSB's retail brokers. appraisal style comments from retail brokers included "investment banker or research analyst? He should be fired" and "how can an analyst be so wrong and still keep his job?" and "Grubman has made fortune for himself and for the investment banking division. However his investment recommendations have impoverished the portfolio of my clients".

Under the Global Analyst Research Settlement Grubman was censured, permanently barred from the industry and paid US\$15mio in fines and disgorgement for alleged violation of federal securities laws and regulations.

A number of aspects characterised the Spitzer investigation. Traditionally, the domain of securities regulators (e.g. the SEC) and self regulatory organisations (SROs) Spitzer asserted jurisdiction via a 1921 New York business law - the Martin Act which allowed him to investigate financial fraud in the state with sweeping powers and almost complete carte blanche in the conduct of the investigation. He pursued the matters aggressively, in particular subpoenaing huge amounts of emails from Wall Street firms and inevitably finding 'smoking guns' amongst the hundreds of thousands of documents. Spitzer pursued the investigation with zeal including using the media and publicly disclosing 'smoking gun' emails and bad facts. It is important to remember that such investigations are conducted not by impartial fact-gatherers but by prosecutors who will use every lawful means to build and win their case; and "winning the case" may not mean preparing to argue the facts before a jury, but to place such pressure on a firm and its executives that they will simply agree to settle.

Almost all of the facts relied upon in the evidence underlying the global settlement agreement and throughout the Spitzer investigation stems directly from emails and is often simply quoted verbatim. This underscores the need for great care in writing and sending emails. Email represents an almost permanent record, emails can be produced and reviewed in their thousands - and often years later - by those seeking evidence of crimes.

Merrill had policies and procedures which ostensibly

sought to separate Investment Banking and Research and ensure the independence of the latter. It seems clear with hindsight and from the email evidence produced in the investigation that in practice such policies and procedures were either poorly understood or simply not followed. It also seems evident that from time to time management was concerned about the inevitable tensions that were thrown up by the steady drift over time of aspects of research to servicing investment bankers and their lucrative clients. Although it seems that little practically was done to address the obvious tensions and conflicts created.

Finally, in testifying before a US Senate committee hearing on Corporate Governance in 2002 Spitzer commented: "remarkably, throughout our investigation (of Merrill Lynch) which has now led us to examine documents of a significant number of companies there is absolutely no evidence that any compliance department ever took action to stop behaviour that clearly violated internal rules and state and federal law. The failure of the industry's much vaunted compliance structure is appalling.

Special Focus 5 Mutual Fund Scandal

2003 - US\$3bio+¹⁹
Agencies: NYAG, SEC



On 3 September 2003, New York Attorney General Elliot Spitzer, flushed with success in the Dot-Com Research cases (see above) turned his attention to US mutual funds and to certain practices he thought were outlawed. The September 2003 action was targeted at Edward J. Stern ("Stern")

and his investment vehicle Canary Capital Partners, LLC ("Canary"). The complaint alleged that from 1999 to 2003, Canary had engaged in two fraudulent schemes – namely, late trading of mutual fund shares, and market timing of mutual fund shares, generating benefits to the tune of tens of millions of dollars.

The complaint held that these schemes required the knowledge, support and cooperation of certain mutual fund companies owned or operated by well known financial services organisations – specifically, Bank of America, Bank One, Janus and Strong Capital Management. Spitzer's cen-

tral contentions were that the fund management and related companies had reached agreements with Canary to make possible two forms of abuse by Canary – “late trading” of mutual fund shares and short term “timing” trading within mutual funds.

Mutual funds are investment portfolios run in bulk form for and on behalf of a population of underlying investors. As such they are also known as “collective investment schemes”. In the US they are governed by the Investment Companies Act, and their managers by the Investment Advisers Act, both dating back to the fall out from the Great Depression. Interests in these investment portfolios are represented by shares. Such shares are not bought and sold continuously but may only be acquired and disposed of typically daily, on the basis of a set reference price deriving from a valuation of the portfolio as of a specific date and time. To prevent abuse, the time by when an order must be received should precede the valuation point, normally by 2 hours or so. Accepting orders after the valuation point gives the investor the chance to factor in market data not available to others lodging an order by the earlier cut-off point – this information advantage could, for particular circumstances and markets, lead to close to “sure thing” profits. Late trading is contrary to the fund prospectuses and is also illegal.

Mutual funds are typically intended to provide exposure to a particular investment market over a period of time i.e. a “buy and hold” strategy - and are described as such in prospectuses. To generate substantial trading revenues through late trading and other means, higher frequency buying and selling is required. Such buying and selling is inconsistent with the profile of the typical mutual fund investor. It generates transaction and other costs, and is generally distracting in relation to the core investment management activity. Prospectuses typically noted that funds were not intended for such timing strategies and managers typically had the power to reject timers’ orders.

The banks behind the fund management companies were allegedly motivated to strengthen what they saw as an important relationship. In some cases they allegedly participated in trading profits arising. The mutual funds enjoyed greater assets under management and levied higher fees as a result.

Stern was the son of billionaire Leonard Stern, owner of the pet supply giant Hartz Mountain Inc. and was assigned the job of overseeing the family’s money. With this role, he ran Canary, a “hedge fund” type enterprise. Stern, while recognised as extremely bright, was educated as an arts major, not an obvious training ground for such a business role. However his mutual fund timing and late trading strategies were an astounding “success”. According to Spitzer’s complaint, Canary engaged with several institutions to agree the basis

on which it could execute market timing and late trading strategies within their mutual fund ranges. These arrangements included waiving short term redemption fees and agreeing to accept orders after the trade cut-off. Considerable lengths were pursued to provide administrative support – for example installing Bank of America’s trading system at Canary’s offices. There were some offers made in return – for example Canary agreed to leave “sticky” assets elsewhere within Bank of America. The complaint is littered with examples indicating a confused philosophy and approach to this activity. Timers were recognised as discouraged but allowances made for this “special relationship”. In making these allowances the impact on the other mutual fund investors was not usually front and centre, if it existed at all. The considerations were mostly to balance the administrative effort with the overall benefit of the relationship to the banks. Whilst the key point – the impact on other fund shareholders – was identified by some, most of the players cited in the complaint generally seemed to have missed the point completely.

Complicity was not confined to broader relationship points. In one case – Strong Capital – Canary agreed to pay increased management fees as well as a share of Canary’s trading profits. The content of the fund prospectuses run through Spitzer’s complaint. These correctly identify the risks of higher frequency traders and provide powers to reject or expel timers, charge additional levies and so forth. Canary’s trading strategies extended in the falling markets in the early 2000s to synthetically creating shorting strategies for mutual funds. These could only be effected through the manager providing a level of transparency to Canary in terms of positions held within the fund. Such information was not available to other investors, another breach of the basic principle of acting in the collective interests of the investors as a whole.

Spitzer sought to convert civil proceedings and settlements into criminal prosecutions. However his attempt to convince a jury in the case of Theodore Sipholt III, a broker with Bank of America who introduced Canary to the bank, failed and no further cases went to trial. The 3 September 2003 complaint was followed by a long litany of related actions taken by Spitzer, often in conjunction with the SEC, against the “great and the good” of the US mutual funds industry, including (in addition to the parties cited in the Canary case) Invesco, Putnam, CIBC, and Bear Sterns. The campaign generated over US\$3bio in fines and disgorgement of profits, secured from a wide range of institutions over a period of several years. Administratively expensive processes were also imposed to deliver investor compensation.

Spitzer’s market timing campaign was remarkable in terms of the intensity of the spotlight directed at the failure of the

industry to live and breathe fiduciary and similar obligations owed to the underlying mutual fund investors. It is striking that the implications for other mutual fund investors of excessive short term trading – in addition to the illegal late trading - were clearly understood, since fund prospectuses dealt specifically with these aspects. There were, for example, provisions to levy special redemption penalties for short term redemptions, designed to offset the costs involved to facilitate acquisition and liquidation of the underlying mutual fund securities. To facilitate effective trading results, the banks overlooked or disapplicated these protections. For example, redemption fees were waived.

The transcripts cited in the Spitzer complaint illustrate the level of institutional confusion and the inability to focus sufficiently on the duties owed, and rights accruing to, the long term buy and hold investors for whom the funds were designed and run. For example “...we won’t actively seek timers, but when pressed and when we believe allowing a limited/ controlled amount of timing activity will be in [bank’s] best interests (increased profitability to the firm) we will make exceptions under these parameters”.

The specific changes in industry governance that ensued from it were significant and included the requirement for mutual fund boards to be comprised of 75% independent directors, and to appoint a chief compliance officer, answerable to the mutual fund board. However, the fundamental refocusing of the industry on its fiduciary obligations was profound, consistent with the extent of the practice – or poor performance in policing it – that had developed in the US mutual fund industry.

As David D. Brown IV, chief of the investment protection bureau for the New York Attorney General remarked at an early stage post the Canary case breaking, “We continue to be surprised by the depth and breadth of this scandal as well as the amount of money that is involved”.

GLG Partners
2003 - £750,000²⁰
Agency: UK FSA

GLG Partners LP (GLG) and Mr Philippe Jabre were each fined £750,000 for market abuse and breaching FSA principles. Mr Jabre, a managing director of GLG, was given confidential information but breached this restriction by trading on the basis of this information. The FSA found that “GLG is also responsible for Mr Jabre’s market abuse. Firms are accountable for the behaviour of their employees, particularly if they are at a senior level.” For more details see the case of Philippe Jabre in Part 2, Section 7, Criminal Cases above.

Citigroup Japan
2004 - closure of PB Operations^{21/22}
Agency: JFSA

On 17 September 2004, Citigroup was ordered to shut its private banking operations in Japan for breaking banking laws. Their License was revoked for a series of “serious violations,” including manipulative sales practices and a failure to screen out money laundering. Its closure was one of the harshest punishments issued to a foreign financial firm in Japan. The bank apologised, saying six staff including three managing directors had been fired and a further eight reprimanded and asked to leave. Citigroup also ousted three top New York executives over the scandal, including its Vice Chairman, Deryck Maughan. Citigroup boss Charles Prince made a personal and public apology in October repeated by Mr. Peterson, Citigroup’s Japan chief executive. Mr. Peterson told a parliamentary finance committee that lax corporate governance and an “aggressive sales culture” were the cause of the abuses. “What’s very important now is that we learn from those mistakes,” he said. Japanese lawmakers grilled Mr. Peterson over the failure of Citigroup’s internal controls and one committee member suggested the bank should have been slapped with criminal penalties. Under a clean-up plan submitted to Japan’s Financial Services Agency (FSA), the bank pledged tighter integration and local control of its Japanese units. The FSA stated that “it also allowed transactions which “could be suspected of being associated with money laundering”, and “In a management environment in which profits are given undue importance by the bank’s headquarters, a law evading sales system that disregards the laws and regulations of Japan was constructed”. Bank staff and managers, it added, had “obstructed inspectors”, while responses to official inquiries “differed from the truth.”

Citigroup UK
2004 - £14mio (US\$19mio)²³
Agency: UK FSA

In August 2004, the banking giant Citigroup did something that was both very clever and also very stupid. Its European bond trading group executed a short sale on Eurozone government bonds. That sounds simple enough, but this particular market play targeted 119 different bonds across 11 trading platforms. The bank used a computer programme, known to its traders as “Dr Evil”, to stun the market with 188 simultaneous sell orders. The idea was to drive down the price of the bonds, and then buy them back when they were cheaper. The strategy worked and the bank made €15mio. The bank had made money but in the process, a certain amount of panic was caused in the markets. Regulators - and criminal authorities - across Europe looked

at what the bank had done. The UK's FSA described the failings as "very serious" and hit it with a fine. The bank's chief executive, Charles Prince, used more direct language - the traders had been "knuckleheaded", he said. Citi's business was affected, for example, even two years later, Citi had arranged only 2.3% of the debt sold by European Governments down from 10.1% at the time of the Dr Evil trades. The FSA led the regulatory action against Citigroup, because the questionable trades took place in London. It found that the bank had failed to conduct its business with due skill, care and diligence, and failed to exercise proper controls over its London-based bond trading team. Citigroup had failed to achieve the high standards expected from a bank of its size, the FSA said. It had also failed to put adequate risk management systems in place. However, the regulator stopped short of finding Citigroup guilty of the much more serious offence of market manipulation and made no findings against any individuals. The market authorities across Europe conducted their own investigations into what Citigroup had done. Regulators in France, Spain, Ireland and Greece decided to take no disciplinary action. The Italian and German regulators considered that there was a potential case to answer for market manipulation, which was a crime in both jurisdictions. But neither had the power to take criminal proceedings and referred the matter to their local criminal prosecutors.

AmSouth

2004 - US\$50mio (US\$40mio DPA forfeiture; US\$10mio CMP)^{24/25}

Agencies: DoJ – DPA; FinCEN and Federal Reserve Board – concurrent CMP; concurrent C&D from FRB and Alabama Superintendent of Banks

In 2004, a US bank based in Birmingham, Alabama, AmSouth Bank, was cited for wilful violation of the anti-money laundering programme and filing of suspicious activity report (SAR) requirements of the Bank Secrecy Act (BSA). The US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) found the Bank's AML programme lacked adequate board and management oversight; had deficient internal controls that lacked sufficient policies and procedures across the Bank to provide for appropriate due diligence and capture of suspicious activity; lacked adequate training to ensure compliance; and had a materially deficient internal audit process that failed to detect these inadequacies. The failure to include in policies and procedures information about identification of suspicious activity and the procedures to be followed when such an event was identified led to several employees operating under the misconception that suspicious activity reports did not have to be filed unless there was a loss to the Bank. In one such case, as sighted by FinCEN's Assessment

of Civil Money Penalty, the CFO of an AmSouth corporate customer embezzled several million dollars from the corporation over three years using forged and improperly authorised cheques. Although Bank employees noticed that the CFO was conducting a number of highly suspicious transactions, the Bank did not file a SAR because it suffered no loss. Absence of adequate board and management oversight led to a defunct system of communication between departments related to suspicious activity. The legal department had no system in place to alert BSA compliance personnel to subpoenas; litigation activity correlating to suspicious activity; and information requests it received from law enforcement. Further, the Bank ignored red flags, including concerns communicated to Bank management by several employees at various Bank branches indicating accounts were being used in furtherance of a Ponzi scheme. Despite such warnings, the Bank failed to file a SAR until two years after it knew about the suspicious nature of the activity, which led to customers at the Bank losing millions of dollars and eventually the Bank paying tens of millions of dollars in forfeitures. Due to the wilful violation of and the systemic deficiencies in the AML programme, the Bank paid US\$50mio in asset forfeitures and fines to US regulators and the Federal Reserve and entered into a three year Deferred Prosecution Agreement (DPA) with the US Department of Justice (DoJ). This was one of the first cases where the DoJ got involved alongside regulators and started DPAs for banks as well as the issuance of large fines. Not only were severe monetary penalties levied on the Bank but AmSouth's ambitious expansion plan to open 64 new branches had to be delayed for approximately one year because the Federal Reserve restricted the bank's expansion activities until AmSouth complied with AML laws. In May 2006, AmSouth announced they were merging with Regions Bank, which was completed in October 2006.

Special Focus 6

Riggs Bank

2004 - US\$25mio²⁶

Agencies: FinCEN, OCC, FRB – C&D

The first incarnation of Riggs Bank ("Riggs") was in 1836 when William Wilson Corcoran opened a small brokerage house. It expanded in 1840, when Corcoran and George Washington Riggs formed "Corcoran and Riggs", which offered checking and depositing services. Based in Washington, D.C., Riggs was the oldest bank in Washington and was the banker to President Abraham Lincoln. It financed Samuel Morse's invention

of the telegraph in 1845 and also lent US\$16mio to the US government to pay for the Mexican-American War in 1847. In 1868, it provided US\$7.2mio in gold towards the purchase of Alaska and helped finance the expansion of the Capitol Building in the 1860s. Riggs continued to be a prominent financial presence in Washington, known for its esteemed Embassy Banking business, and as of 31 December 2003, Riggs had assets of approximately US\$6bio, deposits of US\$4.29bio, and stockholder's equity of US\$472.2mio.

To associate money laundering and foreign corruption with such an institution seemed incredulous but that is exactly what happened in May 2004 when Riggs was fined US\$25mio by the US Department of the Treasury for willful violations of the Bank Secrecy Act of 1970 ("BSA"). The day after this fine, the Federal Reserve Board issued a cease and desist order to stop deficient anti-money laundering ("AML") practices and Riggs consented to the issuance of the order. On 16 May 2005, the Riggs name was officially retired when it was acquired by PNC Financial Services. PNC phased out the troubled Embassy Banking business that was once home to most embassies in Washington.

Investigations by bank regulators led by the Office of the Comptroller of the Currency ("OCC"), Riggs' primary federal supervisory agency, and hearings held by the US Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs determined that Riggs wilfully violated the suspicious activity, currency transaction reporting and anti-money laundering programme requirements of the BSA and its implementing regulations.

The investigation revealed significant deficiencies in Riggs' AML programme. Riggs Bank in Washington DC was cited for wilful violation of the suspicious activity and currency transaction reporting, as well as the AML programme requirements of the BSA and its regulations. Specific problems listed included: Internal controls that were inadequate to ensure ongoing compliance with the BSA across business lines. They were not designed for the high-risk customers, products, services and international reach of the bank's business; Risk matrices used in some of Riggs' divisions contained similar criteria (not tailored to line of business on a risk-graded basis); The bank's customer due diligence programme was not implemented in all areas consistently. The bank consequently failed to identify a large number of accounts associated with two foreign governments. Enhanced due diligence was inadequate in some high-risk areas, such as: Pay on ID wire transfers; Dealings with cheque cashers and money remitters; International private banking;

Embassy banking; and Banking with politically exposed persons and non-resident aliens. Controls inadequate to identify suspicious transactions or to ensure timely filing of complete SARs; Failure to ensure that subpoenas and other government requests were referred for investigation potential suspicious activity; Failure to effectively manage its largest banking relationship, which involved a foreign government's accounts and politically exposed persons, and companies owned by those persons, in spite of warnings; Failure to have effective independent testing of the bank's BSA compliance since internal audit could not verify the effectiveness or timeliness of management's corrective actions for identified deficiencies and the scope of audit omitted areas of money laundering vulnerabilities, BSA compliance or SAR process; BSA management was ineffective in day-to-day oversight, development and application of measures for compliance; Inadequate training on monitoring and detecting suspicious activity; Failure to make timely filing of 33 SARs covering US\$98mio in suspicious transactions. Some SAR filings were delayed two or three years because subpoenas and other matters were not referred for investigation. Other late SARs related to failure to detect regular structuring of cash deposits and money order purchases; when SARs were finally filed, they were deficient; Failure to detect and report suspicious cash, monetary instrument and wire activity by the governments of two foreign countries, their politically-exposed persons, and their companies. In one case, the bank's relationship manager had signature authority on two accounts within the relationship. This manager was inadequately supervised by the bank and as a result the manager engaged in suspicious transactions himself, including the alteration of a cheque, and over US\$1mio in wire transfers into the manager's private investment corporation account at another bank; Filing of CTRs on transactions of two markets under incorrect names, involving 142 CTRs covering US\$7.3mio dollars; Filing of CTRs on accounts of a business owned by a politically exposed person with an incorrect line of business, including transactions totaling US\$11.5mio.

These included an inability to compile information on all of the accounts related to a specific client, inadequate information on client backgrounds and the source of wealth in client accounts, a failure to identify high risk accounts, inadequate monitoring of client transactions, inadequate systems for reporting suspicious activity to law enforcement, weak supervision of account managers, and weak leadership within the bank concerning the importance of AML efforts. These deficiencies led to the mishandling of accounts held by prominent foreign government officials all while the bank shared the same prestigious street address as the

White House and the Department of the Treasury. The more egregious conduct was found in Riggs' handling of accounts for Augusto Pinochet and government officials for Equatorial Guinea.

The investigation determined that Riggs served as the long-standing private bank for Augusto Pinochet, former President of Chile, and deliberately assisted him in the concealment and movement of his funds while he was under investigation and the subject of a world-wide court order freezing his assets. The Pinochet accounts were the fourth largest in Riggs' International Private Banking Department.

After taking power in a 1973 coup, Pinochet served as President of Chile until 1990 and as Commander-in-Chief of the Chilean army until 1998. After stepping down from the army, he became a "Senator for life." Since the first days of his regime, Pinochet was accused of human rights violations, torture, assassinations, death squads, drug trafficking, arms sales, and corruption, but was never convicted in a court of law. Since 1996, he has been the subject of repeated litigation in Spain, the UK, Chile, and other countries for crimes committed during his presidency. In each case to date, he has been found by the presiding court to be unavailable, unfit, or immune to prosecution.

Between 1994 and 2002, Pinochet maintained accounts with Riggs with assets ranging from US\$4-8mio. Riggs opened multiple accounts and accepted millions of dollars in deposits from Pinochet with no serious inquiry into his source of his wealth. The more egregious conduct centred on Riggs' active measures to assist Pinochet in concealing his ownership/control over his funds, and in the movement of his funds. These efforts included: establishment of offshore shell corporations, and then the opening of accounts for said entities; after a media report that Pinochet had over US\$1mio in an account at Riggs, the names on the personal account controlled by Pinochet in the US, were changed from "Augusto Pinochet Ugarte & Lucia Hiriart de Pinochet" to "L. Hiriart &/or A. Ugarte." Thus, Riggs ensured that any manual or electronic search for the name "Pinochet" would not identify any accounts at the bank; transferred US\$1.6mio from a London account to the US while Pinochet was in detention and the subject of a court order freezing his accounts; conducted transactions through Riggs' own accounts; and issuing eight, sequentially numbered, cashier's cheques payable to Augusto Pinochet, each in the amount of US\$50,000. Riggs then sent a banker to Chile to hand deliver the cheques to Pinochet. Riggs repeated these actions, ultimately transferring US\$1.9mio to Pinochet in Chile through cashier's

cheques.

Contrary to Riggs' policy statements requiring detailed "know your customer" ("KYC") information for its client accounts, Riggs did not conduct thorough due diligence to ensure that Pinochet had accumulated his wealth through legitimate means nor did the bank obtain information from him. While Riggs did have KYC documentation for some accounts, the provided information was brief, incomplete, and, at times, misleading. One of the client profiles prepared for the offshore shell corporations listed the beneficial owner's name as "Kept in Vault."

It was also determined that Riggs failed to identify or report suspicious account activity and concealed the existence of the Pinochet accounts from OCC bank examiners for two years. Moreover, Riggs omitted the Pinochet accounts from the OCC in response to a request for a list of accounts controlled by foreign political figures. Even after examiners found some Pinochet accounts through a random sampling of KYC data, Riggs failed to disclose that Pinochet was the beneficial owner. During a subsequent exam, the OCC finally discovered the Pinochet accounts. Riggs was one of more than two dozen banks chosen to undergo this targeted examination. It was during this examination that OCC examiners came across coded references in a Riggs' log of cashier's cheques, asked Riggs for an explanation, and learned of the Pinochet accounts.

In 2002, after a detailed examination, the OCC presented its findings on the Pinochet accounts to the Riggs Board of Directors and Riggs finally closed the Pinochet accounts. It is worth noting that the OCC "examiner in charge" (EIC) of Riggs from 1998 to 2002, the years regulators and federal law enforcement officials at Treasury say the bank repeatedly violated anti-money laundering rules, left the government in 2002 to join Riggs Bank as a vice president. A review was launched at the OCC in 2004 to determine why the years-long abuses at Riggs went uncorrected for so long as well as to probe issues surrounding the EIC's conduct to determine whether the bank exerted "inappropriate influence" on regulators and when the bank offered the EIC employment. In February 2005, the bank and the Allbritton family agreed to pay US\$9mio to Pinochet victims for concealing and illegally facilitating movement of Pinochet money out of Britain.

The disclosure of the Pinochet accounts and the actions he took to conceal his funds led to a re-examination of criminal charges. Pinochet was found competent to face charges, but died before any trial. In September 2007, however, Pinochet's widow and five children were

charged by a Chilean court on charges that included embezzlement.

Investigations into Riggs Bank also found that, from 1995 to 2004, Riggs Bank administered more than 60 accounts and certificates of deposit for the government of Equatorial Guinea (E.G.), E.G. government officials, or their family members. The E.G. accounts represented the largest relationship at Riggs Bank, with aggregate deposits ranging from US\$400-700mio at a time. It was revealed that Riggs Bank serviced the E.G. accounts with little or no attention to the bank's AML obligations. Despite evidence suggesting that Riggs was handling the proceeds of foreign corruption, Riggs allowed numerous suspicious transactions to take place without notifying law enforcement.

Riggs opened multiple personal accounts for the President of E.G., Teodoro Obiang, his wife, and other relatives; helped establish offshore shell corporations for the E.G. President and his sons; and over the course of three years, facilitated nearly US\$13mio in cash deposits into Riggs accounts controlled by the E.G. President and his wife. In addition, Riggs opened an account for the E.G. government to receive funds from oil companies doing business in E.G., under terms allowing withdrawals with two signatures, one from the E.G. President and the other from either his son or his nephew. Riggs subsequently allowed wire transfers withdrawing more than US\$35mio from the E.G. government account, wiring the funds to two companies which were unknown to the bank and had accounts in jurisdictions with bank secrecy laws. Riggs failed to report any suspicious activity in the E.G. accounts.

Riggs' violations of the BSA were systemic and its AML programme had long-standing major deficiencies. Riggs' failures resulted in irreparable franchise damage because of its actions of being the bank for corrupt foreign political officials. The rules underlying the handling of politically exposed persons or PEP relationships were reinforced and served as an important lesson for their regulatory justifications as a means of deterring public corruption. In effect, Riggs Bank became the model in how not to handle PEP relationships. By failing to properly conduct requisite enhanced due diligence, and its concealment efforts, it undermined Riggs' ability to conduct meaningful surveillance on high risk accounts and was unable to fulfill its SAR filing obligations.

Further, the flaws in Riggs' AML programme were repeatedly identified in regulatory examinations and internal audits, and Riggs repeatedly promised to correct them, but failed to do so. Thus underscoring the need to ensure such serious issues are tracked for corrective

actions by a control function such as audit.

Oppenheimer & Company

2005 - US\$2.8mio³¹

Agencies: FinCEN, New York Stock Exchange (examining authority)

Oppenheimer is a securities broker dealer in New York. It was cited for deficiencies in its anti-money laundering programme and resulting failure to identify and report suspicious transactions, during the period from April 2002 through 2004. Specific problems listed included: inadequate internal controls for ensuring compliance with the BSA and implementing regulations, especially those requiring SARs; failure to detect and report suspicious journal transactions and wire transfers in one of Oppenheimer's foreign offices and a Florida office; failure to aggregate wire transfers by customer, account, office or destination to see a true picture of total money movements; failure to review accounts with post office addresses, including a large number of apparently unrelated persons showing the same home or business address (post office boxes or "care of" addresses in Florida); failure to provide for independent testing of BSA compliance, and permitting Internal Audit to play a supervisory role in reporting suspicious activity; failure to adequately staff for coordination and monitoring of BSA compliance. One officer and one analyst, both with other duties, were assigned to this role, when Oppenheimer had 1,600 registered representatives at over 100 branch offices serving 360,000 customers; failure to have a BSA compliance training programme tailored to job responsibilities; failure to timely file SARs involving several million dollars in transactions in 2003; and filing incomplete SARs involving a foreign branch.

Special Focus 7

UBS

2004 - US\$100mio CMP^{27/28/29}

Agencies: US FED

When US marines entered the Central Bank in Iraq shortly after taking the capital city Baghdad by force, they found hundreds of millions of US dollars bundled and bound as if fresh from the US Federal Reserve. This was odd as Iraq had been subject to years of US Sanctions and was blacklisted from much of the international banking system; so how did Iraq acquire these pristine US dollars? Whilst the answer to this question remains likely known to only a few, the find triggered a major response at the Federal Reserve. The FED after being informed and after receiving the serial numbers on the US dollar bills being reasonably freshly cut should be able to identify to whom they supplied these banknotes

from their records and then start to piece together how the freshly cut US dollar banknotes ended up in the vault in the Iraqi Central Bank in Baghdad. In order to ease the introduction and circulation of new US dollar banknotes and to retire old ones, the FED operated a network of relationships with major private sector banks around the world under what is known as the FEDs Extended Custodial Inventory Programme. The FED would establish offshore depots of US dollars with the foreign banks and as a condition, participants in the ECI Programme undertook not to deliver, accept or deposit US dollar banknotes into or out of the NY FED depot to or from clients in countries facing US trade restrictions.

As a result of its enquiries with ECI Programme participants, UBS notified the FED that some deliveries to UBS had been received into the NY FED depot and then taken into UBS possession and then part onward delivered to and/or received from numerous banks in countries such as Yugoslavia, Iran, Libya and Cuba, but not Iraq! UBS also informed that former employees had submitted false reports, covering up the transactions in question. How the US dollars got to Iraq remains in public at least a mystery. As a result, UBS decided to end its banknotes trading business with counterparties in countries outside Switzerland. The Federal Reserve Board and the Swiss Federal Banking Commission also reprimanded UBS. The FED and UBS agreed to a civil liability penalty of US\$100mio for violating the terms of the ECI agreement. There were no findings that UBS actions breached US other Sanctions. Peter Wuffli, then Chief Executive Officer, said: "UBS recognises that very serious mistakes were made. We accept the sanctions, take full responsibility, and would like to express our regret."

Following this incident civil litigation was brought against UBS by terror victims in US courts. For more details see Part 1, Section 3, Sanctions and Embargoes, Rothstein v UBS.

ABN AMRO Bank 2005 - US\$80mio; DPA

Agencies: FinCEN, Federal Reserve System, OFAC, DoJ, NY State Banking Department, Illinois Department of Financial and Professional Regulation, De Nederlandse Bank N.V.

For more details, see Special Focus 17 – Royal Bank of Scotland (former ABN Amro Bank).

City National Bank 2005 - US\$750,000³⁰ **Agency:** OCC

City National Bank in Beverly Hills was cited for failure to comply with BSA compliance programme requirements relating to internal controls and an independent audit function; failure to apply required enhanced due diligence policies, procedures, and controls to detect and report money laundering through private banking accounts of non-US persons, and to detect and report transactions deriving from foreign corruption and involving private banking accounts of politically exposed persons; and failure to make timely SAR filings.

Banco de Chile, New York & Miami Branches 2005 - US\$3mio^{32/33/34}

Agencies: OCC C&D and CMP (New York Branch), FinCEN concurrent CMP (NY and Miami Branches), FED C&D (Miami Branch)

Banco de Chile is headquartered in Santiago, Chile. The New York Branch and Miami Branch of Banco de Chile were cited by FinCEN in October 2005 for failing to establish and maintain an adequate system of internal controls and failing to designate a person, or persons, to adequately ensure compliance with the Bank Secrecy Act (BSA). In addition they also failed to conduct adequate independent testing for compliance with the BSA. All of these failures, along with an inappropriate level of due diligence led to failures by both branches to identify, monitor and report in a timely manner suspicious activity related to prominent Chilean PEPs. FinCEN issued a CMP for US\$3mio to be concurrent with the OCC CMP below. Previously, in February 2005, the New York Branch consented to a Cease and Desist Order with the OCC and the Miami Branch consented to the issuance of a Cease and Desist Order by the Federal Reserve Bank.

The OCC C&D Order required the restructuring of the management and compliance operations at the New York Branch due to the discovery by the OCC that former branch personnel had concealed accounts of Augusto Pinochet, former Chilean dictator, under the names of nominees and others acting under Pinochet's direction. The OCC also identified serious deficiencies in the branch's compliance with the BSA and AML laws and regulations. The branch improperly opened and maintained accounts in contravention of internal policies and procedures and failed to classify and monitor high risk accounts and accounts of PEPs. The OCC discovered that the branch opened accounts without determining the source of funds and failed to scrutinize the purpose of the transactions. Former representatives of the branch allowed millions of dollars in deposits and credits from internal and external transfers

to accounts controlled by persons acting under Pinochet's direction or authorization. These often included circular transactions with no disclosed or apparent legitimate business purpose and without suspicious activity reporting by the branch. The OCC issued a CMP for US\$3mio in October 2005. The FED C&D issued to the Miami Branch referenced many of the same BSA/AML programme deficiencies and focused on the methodology for assigning risk levels to their customer base and enhanced due diligence on higher risk clients and transactions. Significant deficiencies were found in the Miami Branch's policies and procedures for customer due diligence, identification and reporting of suspicious activity, and risk management associated with customer accounts and transactions, as they relate to PEPs.

Pacific National Bank (Banco del Pacifico) 2005 US\$7mio CMP (2010)^{35/36/37}

Agencies: FinCEN CMP, OCC C&D and concurrent CMP

Pacific National Bank, a Miami-based bank that is a subsidiary of Banco del Pacifico S.A., which is owned by the Ecuadorian central bank, paid a US\$7mio civil penalty to Treasury Department agencies in March 2011 for violating a 2005 consent order to beef up its money laundering compliance measures. The OCC and FinCEN jointly assessed the penalty, which was satisfied by one US\$7mio payment to the Treasury Department. Pacific did not admit or deny the allegations, but consented to the payment.

In 2005, Pacific received a consent order to improve its programme as a result of its high risk customer base (85% are from Ecuador), and while the OCC said it "took some necessary steps" to improve, they weren't enough to satisfy the requirements of the order. Specifically, the Bank failed to (i) adequately identify, monitor, and report suspicious activities; (ii) adequately monitor its foreign correspondent bank accounts; (iii) conduct sufficient due diligence; and (iv) adequately audit its high risk areas and the transactions conducted in those areas. "Banks must devote appropriate resources commensurate with their risk profile and must take prompt and necessary steps to comply with the OCC enforcement actions to ensure compliance with the Bank Secrecy Act and the USA Patriot Act," said John Walsh, acting Comptroller of the Currency, in a statement.

FinCEN determined that the Bank failed to implement adequate internal controls and independent testing at a level of consistency necessary to assure compliance with BSA anti-money laundering programme and suspicious activity reporting requirements. The Bank lacked reasonably complete due diligence information for numerous customers, necessary to effectively monitor transactions and report suspicious activity in a timely manner. The Bank violated BSA suspicious activity reporting requirements

by filing numerous suspicious activity reports on a delayed or incomplete basis. "Financial institutions choose their customer base and the geographic areas they wish to serve; those choices drive their regulatory compliance obligations," noted FinCEN Director James H. Freis, Jr. "Regulators must coordinate efforts, as in this case of concurrent actions by FinCEN and the OCC, to address compliance deficiencies and delayed and incomplete reporting pursuant to the BSA."

New York Stock Exchange

2005 - US\$20mio³⁸

Agencies: SEC

The SEC brought enforcement actions against NYSE specialist firms and the NYSE itself in connection with violations of securities laws and NYSE rules which prohibit specialists from "inter-positioning" and "trading ahead" of customer orders. Specifically, the SEC found that from 1999 through 2003, NYSE specialists repeatedly engaged in unlawful proprietary trading, resulting in more than US\$158mio in improper gains. The improper trading took various forms, including "inter-positioning" the firms' dealer accounts between customer orders and "trading ahead" for their own accounts in front of executable customer orders. The NYSE was criticised for failing to adequately monitor and police specialist trading activity, allowing the vast majority of this unlawful conduct to continue. The illegal trading went largely undetected because the NYSE's regulatory programme was deficient in surveilling, investigating and disciplining the specialists' trading violations. The NYSE agreed to several significant remedial measures designed to strengthen the NYSE's oversight of specialists and other floor members. The NYSE agreed to an undertaking of US\$20mio to fund regulatory audits of the NYSE's regulatory programme every two years through the year 2011 and to improve their monitoring and surveillance.

Arab Bank

2005 - US\$24mio CMP – shutdown US\$ wire transfer business and Insured Bank³⁹⁻⁴⁴

Agencies: FinCEN CMP, OCC concurrent CMP

In 2005, the Financial Crimes Enforcement Network and the Office of the Comptroller of the Currency determined that the New York Branch of Arab Bank had inadequate programmes to prevent money laundering and terrorist financing, and therefore, failed to comply with the Bank Secrecy Act. The US authorities also found that Arab Bank failed to meet the reporting requirements of the Bank Secrecy Act. As a result the two US agencies each assessed a US\$24mio CMP against the New York Branch of Arab Bank that would be satisfied with a single US\$24mio pay-

ment to the US Department of the Treasury.

In 2004, suicide bombing victims and their families filed a lawsuit against the Jordan-based Arab Bank, alleging that the bank had processed donations from the Saudi Committee in Support of the Al Quds Intifada to militant Palestinian groups, including Hamas and Islamic Jihad. The case is known as Linde v Arab Bank and for more details see Part 1, Section 3, Sanctions and Embargoes above.

Special Focus 8 Banco Delta Asia

2005 - US Patriot Act Section 311 designation effectively limits ability to operate US\$ accounts/ transactions⁴⁵

Agency: FinCEN

Banco Delta Asia (BDA) was the 10th largest bank in the Chinese gambling enclave of Macao founded in 1935 and owned and controlled by Macau businessman, Stanley Au, with eight branches and 150 employees. In September 2005, the US accused BDA of links to the government of North Korea, and warned of the impending imposition of Sanctions against the Bank, which not only triggered a run on the bank but also led to an investigation by the Macau Government into the affair. The US claimed that the bank had provided financial services, including operating bank accounts and helping front companies by facilitating wire transfers, for more than 20 years to multiple North Korean-related individuals and entities that were engaged in illicit activities, without providing details of what such illicit activities were. It claimed that the entities paid a fee to BDA for their access to the bank. It is speculated that the US believed that BDA had long handled trade and financial transactions, including sales of gold bullion, for a range of North Korean government companies and entities (none of which would have been illegal in Macau) but of more concern that BDA was a "willing pawn" in North Korean money laundering and counterfeit-currency trafficking.

Since the end of the Korean War, the US has been inventive in applying pressure on North Korea. It has imposed an arms embargo, economic sanctions, restrictions on trade and travel, bans on dealing with North Korean companies and even a ban on US citizens owning or operating ships flying North Korean flags. Most of these measures have led to some pain, but nothing stung as much as the 2005 action against BDA. The Macau government invoked a banking law to replace BDA's board by government appointees and

after identifying several North Korean companies which had accounts with BDA, froze their accounts affecting US\$25mio. It was well known that North Korean companies banked in Macau with many of the Macau Banks as well as in Mainland China. It was also well known that Kim Jong Nam, the eldest son of North Korea's then leader Kim Jong Il, lived in Macau since 2004.

Stanley Au the owner and Chairman, first learned that his bank was being charged as a bank engaged in "illicit activities" when he saw a report in the Asian Wall Street Journal in September 2005 that his bank was a candidate for a US money laundering blacklist. This "news came as a bolt out of the blue" he would say as BDA had never been informed by the US that its practices were a cause of any money laundering concern. In fact according to Stanley Au, he had only had good relations with the US to this date for example in June 1994 he had provided the US with vital information on North Korea and its counterfeiting US dollars and was told it was okay to continue to do business with the North Koreans at that time. Stanley Au at all times pleaded his and BDA's innocence. Stanley Au maintains that BDA did not charge a fee for its services nor did it conduct illicit services for North Korea or any other customer.

The Bank was only one of the banks in Macau that did business with North Korea. The business his bank had with North Korea began in the mid 1970s and was to assist North Korea with its foreign trade transactions. Also Au described North Korea as a gold producing country and that in the late 1990s BDA had acted as a "gold bullion trader on behalf of the North Koreans". Also BDA bought or sold foreign currency notes for North Korea, including US dollars, because North Korea had a limited banking system and so it couldn't do such transactions itself. Stanley Au petitioned the US challenging the findings against BDA suggesting that BDA was targeted not because of any "voluminous" evidence of money laundering but "because it was an easy target in the sense that it was not so large that its failure would bring down the financial system."

Following the Macau governments intervention into BDA, they found no illegal activity, no criminal charges were filed and BDA was returned to previous management by owner Stanley Au in 2007. Furthermore, an audit by Ernst & Young commissioned by the Macao government found no evidence that BDA had facilitated money laundering.

Notwithstanding this, BDA remains blacklisted by the

US with the 2005 allegations being formalised and a Final Rule of the designation occurring in 2007.

David Ascher, who had been the coordinator for the Bush Administration working group on North Korea and a senior adviser in East Asian affairs in the State Department, in testimony to the US House Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade on 18 April 2007, explained why BDA was chosen to be blacklisted from the international banking system. "Banco Delta was a symbolic target. We were trying to kill the chicken to scare the monkeys. And the monkeys were big Chinese banks doing business in North Korea...and we're not talking about tens of millions, we're talking hundreds of millions."

Whilst the action against BDA made headlines, and no doubt led to greater isolation for North Korea, particularly with Banks that needed to operate internationally, the action also became a major disruption in the so called "six party talks" which were trying to find a way to address the North Korean nuclear weapons programme. The North Koreans were adamant that they wanted their US\$25mio back that was frozen at BDA. North Korea said that the denuclearization and other aspects of the six-party talks can only go forward when the BDA situation is resolved. "To make the money transfer possible freely just like before has been our demand...from the beginning," a spokesperson from North Korea said. The US State Department stated that, "We all want to see the BDA issue resolved, obviously resolved within the laws and regulations of the US as well as the international financial system, and we'd like to move on and get back to the business of the six-party talks, which is really focused on the issue of denuclearizing the Korean Peninsula."

In the end the US, under pressure, agreed to find a way to return the monies frozen with the Macau government and authorized Wachovia Bank in the US as correspondent Bank to BDA to transfer equivalent funds from the BDA correspondent account to North Korea.

The move against BDA demonstrated the power of financial sanctions and of the use of S.311 of the US Patriot Act. Section 311 allows the US to rule that foreign banks, jurisdictions, transactions or accounts are of "primary money laundering concern" and require American financial institutions to take protective measures, including cutting ties with these entities. Non-American Banks often follow such announcements in cutting ties as well.

"Not only did North Korea lose access to this particular financial institution," said Marcus Noland, an authority on the North Korean economy at the Washington-based Peterson Institute of International Economics, "other financial institutions began severing their ties with North Korea, not wanting to risk entanglement in North Korean illicit activities and possible expulsion from US financial markets."

"As a consequence of both these direct and indirect effects," he said, "North Korea has encountered increasing difficulty executing international financial transactions."

The action against BDA has resulted in it being effectively shut out of international banking, without any formal charges being issued or details being provided, without a hearing and despite findings in Macau that there was nothing BDA had done which could be considered illegal.

Special Focus 9 Bank Of New York

2005 - US\$38mio penalties and victim compensation; US\$14mio settlement with Russia Federal Customs Service⁴⁶⁻⁵⁰

Agencies: FED, NY State Banking Department, DoJ NPA

Russian émigrés...money laundering...inside operatives...US\$7.5bio laundered... sounds like a plot from a James Bond movie but unfortunately it was the media headlines that first appeared in August 1999 associated with the US' oldest bank, the Bank of New York (BoNY). This was not the type of press this global financial institution that was established in 1784 by Alexander Hamilton was used to. At the time, BoNY had assets of around US\$67bio and was the 17th largest bank in the country. As the news unfolded over the following weeks and months, it was reported that billions of dollars were channeled through BoNY by Russian organised crime through a major money laundering operation. BoNY ultimately survived this scandal but merged with Mellon Financial Corporation and is now known as The Bank of New York Mellon.

Although a federal grand jury indicted former BoNY vice president Lucy Edwards (born Lyudmila Pritzker) her husband, Peter Berlin, and Aleksey Volkov, along with three unlicensed money transfer companies in September 1999 as part of the 14-month investigation, it was not until February 2000 that the real facts of

the case started emerging. A second former BoNY employee Svetlana Kudryautsev also was indicted for lying to FBI agents. A glimpse at the AML programme enhancements needed at BoNY were revealed when BoNY executed an 8-page Written Agreement with the Federal Reserve Bank of New York (Fed) and the New York State Banking Department in 2005 where it also agreed to a total of US\$38mio in penalties to avoid prosecution for its involvement in this case. BoNY agreed to strengthen its AML policies and procedures and customer due diligence practices in addition to reporting quarterly to the Fed and state regulators on its progress and also about transactions of customers it has identified as potential money launderers. It also agreed to strengthen other areas including risk management, AML oversight, internal audit and automated monitoring to detect suspicious activity. Although the Bank Secrecy Act (BSA) and Suspicious Activity Reports (SAR) existed in 2000, the comprehensive AML Programme regulations introduced by the USA PATRIOT Act were still two years away from becoming effective so the customer due diligence standards and other procedures that we take for granted now did not exist then.

The week following the execution of the Written Agreement, Lucy Edwards and Peter Berlin pleaded guilty to a series of federal crimes, including money laundering, conspiracy to evade income taxes, and bribery of a bank official, and agreed to cooperate with investigators in a plea bargain, in addition to forfeiting over US\$1mio from their personal accounts.

The companies they controlled forfeited around US\$6mio. During their almost 2-hour court appearance, the husband and wife described how between February 1996 and July 1999 more than US\$7bio was sent from Russia illegally and was funneled through network of front company accounts held at BoNY and controlled by Berlin before being transferred to offshore accounts.

As one would expect from a plea bargain, the investigation was far from over as more details were disclosed by Edwards and Berlin and more suspects and money trails were revealed. It was not until November 2005 that this investigation would formally close with BoNY settling with federal regulators for US\$38mio in penalties and victim compensation, and the prosecution of at least nine individuals. BoNY agreed to make what prosecutors described as "sweeping internal reforms to ensure compliance with its antifraud and money laundering obligations." Authorities said that the bank had "accepted responsibility for its criminal conduct" and that it would not be prosecuted as long

as it complied with the terms of the deal for three years. BoNY also agreed to allow an independent examiner to monitor its operations. The Non-Prosecution Agreement (NPA) and financial penalties and compensation also covered an investigation related to the execution of sham escrow agreements by a BoNY branch. For the time being, BoNY had escaped prosecution...at least by the US government. Then in May 2007, Russia filed a US\$22.5bio lawsuit against the bank for money laundering. The suit was subsequently settled for US\$14mio. It's also worth mentioning that in addition to these criminal proceedings, the activity also exposed BoNY to civil liability and a class action suit was filed by its shareholders in August 2000. In addition, a US\$1bio lawsuit was filed by depositors of the defunct Russian bank Inkombank alleging that BoNY helped Inkombank senior managers steal hundreds of millions of dollars by serving as their correspondent bank. These cases were settled for US\$14mio. For more details of this case see Part 2, Section 7, Criminal Cases, Lucy Edwards and Peter Berlin above.

Beach Bank, Miami

2006 - US\$800,000 CMP⁵¹

Agencies: FinCEN, FDIC, Florida Office of Financial Regulation

Beach Bank Miami ("the Bank") agreed to a fine for the failure to implement adequate internal controls to ensure compliance with BSA and manage risks of money laundering. Specific problems listed included: failure to fully investigate activity of three of its 40 MSB customers to determine if it was suspicious. The three collectively withdrew over US\$615mio in cash over 18 months; the Bank received federal subpoenas, so it had knowledge customers were being investigated; the Bank knew of cash activity, because it filed CTRs on it; the Bank failed to review available audits of its MSB customers to monitor risk of potential money laundering in those accounts; Bank failed to monitor its more than 200 identified high risk accounts, in spite of policy to do so; lack of controls to monitor funds transfers for suspicious activity. There was over US\$1bio transferred over 21 months. One telecommunications company moved US\$100mio in two months, but the Bank had no file documents to back up that level of phone card sales and telecom services; and failed to timely file suspicious activity reports. Because of inadequate anti-money laundering procedures, the Bank failed to detect and report on a timely basis on at least 67 cases related to over US\$1.6bio in suspicious activity.

The Foster Bank, Chicago

2006 - US\$2mio CMP⁵²

Agency: FinCEN

The Foster Bank, Chicago agreed to the imposition of the CMP, without an admission of guilt. It was cited for a failure to implement adequate internal controls to ensure compliance with BSA and manage risks of money laundering. Specific problems listed included: the bank issued US\$130mio in cashier's cheques in eight months of 2002, without adequate AML procedures and controls; the bank is located in both a High Intensity Drug Trafficking Area (HIDTA) and a High Risk Money Laundering and Related Financial Crimes Area (HIFCA); the bank failed to have a customer due diligence programme to identify expected or reasonable customer activity; the bank failed to use its large currency transaction log to identify structuring over multiple-day periods; the bank incorrectly exempted two MSBs for at least 18 months. This resulted in the late filing of at least 674 CTRs totalling over US\$35mio in transactions; the bank's independent review of its BSA programme was not adequate. Two outside firms failed to identify the bank's monitoring weaknesses; the scope of the independent BSA review was inadequate, given the high volume of funds transfers to "Jurisdictions of Primary Concern" for money laundering, and the large volume of monetary instrument transactions at the bank; the bank failed at least 12 times to make timely SAR filings. One customer operating a sportswear business structured nearly US\$10mio in cash transactions from April 1999 - November 2002. Another customer routinely made cash deposits of US\$9,900 up to four times a day, with no apparent business purpose. Other customers made large currency transactions of US\$300,000-US\$600,000 per month, some apparently structured, with no apparent legitimate reason; the bank filed SARs that omitted significant relevant information. In one case, the bank failed to include pre-1999 activity involving wires to Pakistan, India, and United Arab Emirates, understating overall dollar volume by US\$22mio. In another, the bank omitted information on daily structuring activity in other customer accounts and the former bank president structured US\$419,000 in bank transactions on behalf of his son's business and US\$122,000 on behalf of a former bank director.

Israel Discount Bank of New York

2006 - US\$12mio⁵³

Agencies: FinCEN, FDIC, NY State Banking Department

Israel Discount Bank Of New York, which is the US subsidiary of Israel Discount Bank Ltd. (Israel), agreed to the imposition of the CMP, without an admission of guilt. The bank was cited for failure to implement adequate internal controls to ensure compliance with BSA and manage risks

of money laundering, and failure to conduct adequate independent testing of its BSA programme, and to adequately staff the compliance function. Specific problems listed included: Deficient documentation of customer information to adequately assess risk for money laundering; failure to link customer accounts with common ownership to facilitate detection of suspicious activity; failure to adequately review documentation for high-risk foreign accounts, such as non-bank financial institutions in Latin America; lack of adequate systems and controls to monitor wire transfers for money laundering or other suspicious activity. In one year, there were 181,000 wires totaling US\$35.4bio, with originators or beneficiaries with money laundering characteristics. In addition, there was a failure to follow up on alerts from an inadequate automated monitoring system; failure to have adequate controls and monitoring procedures over activity in accounts of its own subsidiary, DBLA; independent testing programme was inadequate; Failure to adequately staff its compliance function with persons responsible for monitoring day-to-day compliance with BSA; failure to make timely SAR filings, and failure to monitor on-going activity in accounts it had filed SARs on; filing of incomplete or inaccurate SARs.

Liberty Bank of New York

2006 - US\$600,000 CMP⁵⁴⁻⁵⁷

Agencies: FinCEN, FDIC, NY State Banking Department

In May 2006, the Financial Crimes Enforcement Network (FinCEN), Federal Deposit Insurance Corporation (FDIC), and New York State Banking Department (NYSBD) announced the assessment of civil money penalties totaling \$600,000 against Liberty Bank of New York for violations of federal and state anti-money laundering laws and regulations. Liberty Bank, without admitting or denying the allegations, consented to payment of the civil money penalties.

In taking these actions, FinCEN, FDIC, and NYSBD determined that Liberty Bank failed to implement an adequate BSA/AML programme, with internal controls and appropriate measures to detect and report money laundering and other suspicious activity in a timely manner. They failed to designate anyone to coordinate and monitor day-to-day BSA compliance. There was a lack of adequate policies, procedures and controls for detection and reporting of suspicious transaction as well as a failure to describe responsibility for detecting, evaluating and reporting of suspicious activity. In addition, there was a patchwork and undocumented process for monitoring transaction activity and a failure to obtain enough information on customers, especially those in cash-intensive businesses. All of this in turn led to a failure to make timely SAR filings and a failure to include adequate narrative information in filed SARs.

The agencies also found that systemic defects in Liberty Bank's anti-money laundering programme resulted in a failure to comply with information sharing requests from law enforcement under section 314(a) of the USA PATRIOT Act.

BankAtlantic

2006 - US\$10mio CMP/Forfeiture⁵⁸⁻⁶⁰

Agencies: FinCEN, OTS (C&D), DOJ (DPA)

In April 2006, Florida-based BankAtlantic entered into a deferred prosecution agreement with the US DoJ and forfeited US\$10mio to resolve charges of failing to maintain an anti-money laundering programme. Concurrently, the Office of Thrift Supervision and the Financial Crimes Enforcement Network each assessed a US\$10mio civil penalty against BankAtlantic for violations of the BSA, and both were deemed satisfied by the payment of the US\$10mio forfeiture. The charge filed against BankAtlantic arose out of transactions conducted by and through BankAtlantic between July 1997 and April 2004. During this time, more than US\$50mio in suspicious transactions were conducted through accounts at BankAtlantic, including transactions involving more than US\$10mio of identified drug proceeds. BankAtlantic failed to detect, identify and report the suspicious transactions in the accounts, as required by the BSA. Specifically, an undercover operation by the Drug Enforcement Agency into the laundering of drug proceeds led to the finding that suspected drug money was wire transferred to a handful of accounts at BankAtlantic, managed by a branch manager. Further investigation led to the discovery of other BankAtlantic accounts that were suspected of being used to launder drug money. BankAtlantic admitted that it did not identify and report the suspicious activity occurring in these accounts.

The list of specific problems included: lack of adequate policies, procedures and controls for compliance with BSA and to manage money laundering risk, including the detection and reporting of suspicious transactions; failure to monitor for suspicious activity by not: 1) having adequate systems to monitor wire transfers, 2) ensuring review of subpoenaed accounts, and 3) having systems for detection and reporting of multi-day cash structuring; a branch of the bank catered to high income/net worth individuals, without effective customer due diligence or transaction controls and monitoring; employees were able to initiate large dollar wire transfers without oversight; failure to detect/report suspicious activity by foreign unlicensed MSBs; lack of risk analysis on high-risk clients that included non-resident aliens, offshore businesses, consulates and PEPs; lack of oversight for pouch activity deposits; deficient programme for independent testing of BSA programme, and failure of audit and management to follow up on significant identified deficiencies; failure of the bank's designated BSA com-

pliance officer to monitor and coordinate compliance on an enterprise-wide basis; inadequate job-specific training to ensure BSA compliance; and failure to make timely SAR filings, which impaired the usefulness of those SARs that were filed late. More than 360 SARs were delinquent, covering over US\$189mio in suspicious transactions.

Special Focus 10 American Express Bank International

2007 - US\$65mio CMP/Forfeiture⁶⁴⁻⁶⁶

Agencies: FinCEN CMP, FRB C&D and CMP and DoJ DPA

American Express Bank International (AEBI) is owned by American Express Bank Ltd. (AEB), a New York corporation. AEBI offers private banking services, primarily to high net worth customers in Latin America. American Express Travel Related Services Company (AETRSC) is an MSB. On August 3, 2007, the Federal Reserve Board issued a Cease and Desist Order and a CMP of US\$20mio against AEBI, and FinCEN issued a CMP against AEBI of US\$20mio and against AETRSC of US\$5mio. There is a related Deferred Prosecution Agreement (DPA) and US\$55mio forfeiture order by the Department of Justice (DOJ) against AEBI. Cross-order payment agreements make the total effective charges, including the forfeiture, US\$65mio.

The DOJ in collaboration with the Drug Enforcement Agency (DEA) found that from 1999 through 2004, the bank which primarily offered private banking services to Latin American clients allowed South American customers to use their accounts to process parallel currency exchange market transactions which in many instances turned out to be Black Market Peso Exchanges (BMPE).

According to the DPA, transactions of note were dozens, sometimes hundreds of incoming funds from persons and entities unrelated to the account holder and in many of the cases, the transactions were not consistent with the nature of the client's business. Additionally, as part of the DEA investigation, drug proceeds were transferred to AEBI accounts directly from law enforcement agents, who in an undercover capacity were "working for" Colombian money brokers and drug traffickers.

One of the examples sighted in the DPA was an account controlled by a Colombian national, but held in the

name of an offshore bearer share corporation, which in turn was controlled by three other bearer share corporations, which in turn had given the Colombian national a power of attorney, authorizing him to control the financial affairs and bank accounts of the original bearer share corporation. The individual processed millions of dollars in what appeared to be BMPE transactions through the bank, allowing money brokers access to the funds.

Despite the bank operating in a High Intensity Drug Trafficking Area and providing private banking services to a region known as a source for illegal narcotics, they failed to implement a dynamic AML programme which should have established the true beneficial owner of accounts and risk weight the client population as well as apply increased monitoring scrutiny to those client types or geographic areas which posed heightened risk. These factors coupled with compliance personnel's sole reliance on the private bank relationship manager's explanation of transactions to clear cases led to the breakdown.

Financial institutions can take measures to identify BMPE payments by scrutinizing the remitter of funds used to settle a US transaction as they are usually sent by a third party unrelated to the customer receiving the goods in South America. Indicators of BMPE dollar payments can involve bulk cash deposits, structured money orders, traveller's cheques, cashier's cheques or bank notes under US\$10,000 in value or cheques drawn on US institutions from persons or entities unrelated to the US exporter's client.

In addition to the 2007 DPA, AEBI entered into a settlement agreement with the DOJ in 1994 stemming from an indictment and conviction of two AEBI employees as a result of a US Customs investigation into Juan Garcia Abrego (leader of the Mexican Gulf Cartel). AEBI agreed to penalties and forfeitures of funds in addition to spending no less than US\$3mio on BSA development. In late 2007 AMEX announced the sale of AEBI to Standard Chartered PLC.

Specific findings included: failure to adopt and implement comprehensive customer due diligence and enhanced due diligence processes, particularly regarding high risk customers; failure to maintain effective control measures for bearer share and other PICs; failure to adhere to bank's own written policies requiring periodic reviews of high risk accounts; the bank's transaction monitoring system continued to be inadequate to the task, due to data integrity and other problems. System-identified potentially suspicious activity was not properly resolved, so the bank could not identify, monitor and report suspicious activity; AEBI

did not perform satisfactory independent testing of its BSA/AML programme. In particular, the bank's internal audit function did not review implementation of the bank's automated transaction monitoring system; failure to provide for adequate oversight of and accountability for the BSA/AML compliance programme by management of AEBI and by its parent company, AEB, which had agreed to provide oversight.

The bank agreed to make improvements to its transaction monitoring system and also agreed to an independent review of account and transaction activity for the first half of 2007 to determine whether suspicious activity was properly identified and reported. The order specifically required that the review be completed notwithstanding any agreement to sell AEB or AEBI to an unaffiliated third party.

Union Bank of California

2007 - US\$10mio CMP, US\$21.6mio Forfeiture⁶¹⁻⁶³

Agencies: FinCEN CMP, OCC CMP & C&D and DoJ DPA

Union Bank of California, N.A., is a national bank headquartered in San Francisco. It is a subsidiary of UnionBanCal Corporation, based in San Francisco, which in turn is a majority-owned subsidiary of Mitsubishi UFJ Financial Group, Inc., of Tokyo, Japan. According to the OCC's findings, Union Bank failed to adequately monitor its casa de cambio (Mexican currency exchange) accounts for suspicious activity. Beginning in 2003 and through 2005, the bank failed to timely file hundreds of SARs, which permitted the undetected laundering of millions of dollars of suspected drug trafficking proceeds. On 23 March 2005, Union Bank entered into a Memorandum of Understanding (MOU) with the OCC, requiring implementation of a bank-wide BSA compliance programme, improved internal controls for monitoring high risk accounts and transactions, enhanced training and audit, and enhanced due diligence procedures, particularly regarding private banking customer accounts. In the bank's 2006 BSA compliance exam, the OCC determined that Union Bank had not achieved compliance with the terms of the MOU. The bank's FIU proved ineffective in detecting and reporting suspicious activity because of inadequately trained staff and ineffective oversight. Due diligence controls were insufficient for an effective SAR process. In addition, Fin CEN reported that a review of SARs filed by Union Bank in the 12 months ending January 2006 revealed over 1,000 cases of reporting fields in SAR forms left blank or incorrectly completed. In September 2007, the OCC levied a US\$10mio Civil Money Penalty (CMP) on Union Bank, and issued a C&D replacing its 2005 MOU. FinCEN assessed a separate US\$10mio CMP, but waived collection if the OCC penalty is paid. In a related criminal investigation, the Department of Justice (DoJ) issued a Deferred Prosecution Agreement

and a US\$21.6mio forfeiture order against the bank. DoJ agreed to recommend that its case against the bank be dismissed with prejudice in 12 months, if the bank "fully implements significant anti-money laundering measures required by the agreement." The DPA was terminated in October 2008.

Bank Of America

2007 - US\$10.5mio (US\$3mio CMP (2007) & US\$7.5mio (2006)^{67/68}

Agencies: NY AG, NASD

During the investigation of Beacon Hill Service Corporation and Lespan (see above in Part 2, Section 7, Criminal Cases) by the Manhattan District Attorney's Office, the latter being a money transmitter in Uruguay, focus turned to the transfers by money service businesses (MSBs) of billions of US Dollars through accounts at one of Bank of America's ("BoA") Manhattan branches.

The US investigation was conducted over two years, in which it was revealed that from May 2002 to April 2004, over US\$3bio flowed through Lespan's account at BoA. The case was a collaborative effort between US and Brazilian authorities. In the US, a joint investigation with ICE (Immigrations and Customs Enforcement), New York State Banking Department and Manhattan District Attorney's office led to the indictment of 34 people and 16 British Virgin Island companies for conducting illegal money transfer businesses in New York. Brazilian Federal Police executed over 121 arrest warrants and 215 search-and-seizure warrants in Brazil for money laundering and related tax evasion crimes. Money exchange houses, or doleiros as they are known in Brazil, were able to exchange foreign currency but were prohibited to send funds abroad. Lespan facilitated money transfers without proper documentation or registry with Brazil's central bank. For additional fees, Brazilian clients were able to move money in and out of Brazil without reporting to the government, by simply utilising services provided by doleiros. The illegal transfer services provided by the doleiros, allowed clients to have undeclared assets transferred without any reporting to Brazilian tax authorities. The elaborate scheme required the doleiros to have complex corporate structures whereby they had various related offshore accounts in the Caribbean and used Lespan to transfer clients' money anonymously.

Similar to Beacon Hill, the Lespan accounts were utilised to facilitate payments to the Middle East via the Tri-Border region of Argentina, Brazil, and Paraguay. Historically, this area of South America has a strong connection to the Middle East due to a large concentration of its population of Middle Eastern

origin. Billions of dollars are known to have flowed through the region and some of the monies may have gone to potentially fund terrorist activities. Due to poor recordkeeping; it is difficult to really assess the potential impact that it may have had in funding terrorist activities around the world. Investigators noted too often it encountered cases where the money trail ceased and the ultimate recipient of the funds were never identified. Lespan, through its vast network of accounts at various banking institutions, kept its client identity to a minimum. Since the corresponding banks did not question the flow of funds, it simply remained undetected for years. For its failure in not capturing and reporting the illegal activities of Lespan, BoA was fined US\$6mio to be paid to the City and State of New York; as well as, an additional US\$1.5mio to cover the costs of the investigation. As part of the settlement, BoA recognised its failure to verify and validate information provided by their Latin American MSB clients. By this acknowledgement, it agreed that its internal AML controls were deficient. Furthermore, as part of the agreement, BoA revealed it had taken steps to revise its AML policies, systems and controls and was committed to escalate any new discoveries to Manhattan District Attorney's office and federal regulators.

In a separate concurrent matter, the NASD announced four months after the above-referenced US\$7.5mio settlement that it fined Banc of America Investment Services (BAI) US\$3mio in connection with BAI's "failure to obtain customer information for certain high-risk accounts and for failing to have adequate communication with its parent bank to ensure that BAI's independent suspicious activity report (SAR) filing obligations were met." The penalty was the largest imposed by a US securities regulator for anti-money laundering violations at the time. NASD stated that BAI failed to conform to its own established AML procedures with respect to 34 high-risk accounts involving trust and private investment corporations apparently linked to one family and domiciled in the Isle of Man (noted for its acceptance of offshore banking). While the NASD did not identify the family, the accounts are identical to the Wyly accounts (billionaire Sam Wyly and his brother Charles) as described in an August 2006 report, "Tax Haven Abuses: The Enablers, the Tools and Secrecy," by the US Senate Permanent Subcommittee on Investigations. These accounts engaged in multi-million-dollar international wire transfers. The NASD said the failures defeated the purpose of AML and terrorist financing laws, and came despite in-house warnings from its clearing firm, a senior lawyer and its risk committee to obtain beneficial owner names or to restrict activity if such names were not obtained. In addition, BAI

ignored notices from its clearing firm pointing out indicia of money laundering activity.

International Bank of Miami

2007 – US\$250,000⁶⁹

Agency: OCC

The International Bank of Miami, N.A., Coral Gables, Florida, is alleged to have violated the Bank Secrecy Act; to have engaged in unsafe and unsound practices when it failed to supervise adequately its Capital Markets Group (CMG); and to have failed to ensure that CMG's securities transactions were conducted safely, soundly, and legally.

Specifically, the OCC's order alleges that the bank: violated the BSA and 31 CFR 103.33(a) [records of loan transactions] by permitting CMG to maintain records that frequently failed to adequately identify a legitimate business purpose for loans, or fully and adequately describe the nature and purpose of loans (loans were described merely as being for "working capital"); failed to maintain a system of controls to monitor and report suspicious activity; failed to adequately identify and monitor accounts of politically-exposed persons (PEPs); failed to monitor loans accounts and payments for suspicious activity; did not have an adequate training programme on detecting and reporting suspicious activity; permitted CMG to make loans that did not conform to the bank's own lending policies, and to omit obtaining proper authorization for large credits; allowed CMG to provide incomplete or inadequate loan documentation and recordkeeping, not in accordance with bank policies; failed to do adequate customer due diligence, especially for high-risk customers; allowed CMG to maintain an inadequate record of its securities transactions; permitted OMG to engage in securities transactions in violation of OCC regulations; and allowed CMG to conduct securities transactions with high-risk countries without risk management procedures.

Israel Discount Bank

2008 - NIS 3.7mio CMP⁷⁰

Agency: Bank of Israel

Israel Discount Bank (IDB) is the third largest bank and a leading financial group in Israel. In October 2008, the Israeli Supervisor of Banks announced that it has imposed a fine of NIS 3.7mio on IDB. The AML-related fine was imposed on IDB for deficiencies found during a 2005-2006 Audit by the Bank of Israel.

The Audit findings indicated shortcomings in IDB's obligations with regard to the Anti Money Laundering Act, relating to reporting and documentation requirements for banking corporations, and in accordance with the Anti-Money Laundering regulations pertaining to both the tim-

ing and manner in which a banking corporation is required to report. Two main types of infringement were discovered during the inspection: (a) failure to record identification particulars of beneficiaries and controllers of holding interest, and (b) failure to submit reports or late submission of reports on unusual transactions by customers to the Prohibition of Money Laundering and Financing of Terrorism Authority (IMPA). However, the Banking Corporations Sanctions Committee took into account the fact that IDB acted swiftly to correct the faults revealed during the inspections. The following points were also made. The prohibition on money laundering and financing of terrorism is an intrinsic part of a banking corporation's system of risk management, and a bank must allocate sufficient resources, relative to its size, and the extent and complexity of its activity, to enable the compliance officer (responsible for the prohibition on money laundering) to act so as to ensure the banking corporation meets all its obligations; outsourcing operating functions does not absolve the banking corporation from its obligation to maintain proper oversight, nor does it absolve its management from the responsibility to understand and manage the corporation's risks; the agreement of the banking corporation to carry out customers' wishes that are inconsistent with the legal provisions regarding the prohibition on money laundering and financing of terrorism, even if accompanied by professional counselling, indicates the failure to internalize the issue of the prohibition on money laundering and financing of terrorism, and a defective culture of compliance; and a banking corporation must check whether the declarations by the holders of controlling interests in corporations, including nonprofit organisations, are reasonable.

Mizrahi Tefahot Bank

2008 – C&D; 2011 - US\$350,000 CMP^{71/72}

Agencies: FDIC & California Dept. of Financial Institutions

Mizrahi Tehahot Bank, Ltd., (Mizrahi) is a US branch of an Israeli financial institution, headquartered in Los Angeles. In August 2008, Mizrahi entered into an Order to Cease and Desist with the FDIC and the California Department of Financial Institutions (DFI). Mizrahi was ordered to cease and desist from (a) operating in violation of Bank Secrecy Act ("BSA"), to having an inadequate anti-money laundering programme, requiring improvements to Suspicious Activity Report ("SAR") procedures to identify, monitor, and report suspicious activities; for a lack of due diligence on foreign correspondent accounts. Mizrahi was also ordered to take all necessary steps to ensure future compliance with all applicable laws and regulations, including, but not limited to, Office of Foreign Assets Control ("OFAC") requirements; to provide for a system of internal controls to ensure compliance with the BSA; provide for independent testing of compliance with the BSA, all applicable rules and

regulations related to the BSA, and to have a BSA compliance programme managed by a qualified officer who has the required authority, responsibility, training, resources, and management reporting structure to ensure compliance with Mizrahi's programme requirements and BSA-related regulations; provide and document training by competent staff and/or independent contractors of all of Mizrahi's affected personnel, including, without limitation, senior management, tellers, customer service representatives, lending officers, private and personal banking officers and all other customer contact personnel, in all aspects of regulatory and internal policies and procedures related to the BSA, with a specific concentration on accurate recordkeeping, form completion and the detection and reporting of known and/or suspected criminal activity; review and revise Mizrahi's written customer due diligence programme; develop a programme for reviewing the files of account holders at Mizrahi who have been accorded "W-8" tax exempt status, but who appear to hold such accounts for the benefit of third parties and/or do not qualify for "W-8" tax exempt status; and ensure that it adheres to its existing policy prohibiting acceptance of customers that are Non-Banking Financial Institutions ("NBFI"), which include Money Services Businesses ("MSBs"), or revise its written procedures to include guidelines as to what type of NBFI customers Mizrahi accepts and does not accept and have specific procedures for each.

In January 2011, the FDIC and the DFI issued Mizrahi a US\$350,000 CMP Order, half to be paid to the US Treasury and half to the DFI. The Order stated that the agencies believe that from at least 2000 through 2009, Mizrahi lacked an adequate programme to monitor, analyze, and report suspicious activity. In addition, the FDIC and the DFI have determined that Mizrahi had failed to comply with the August 2008 Consent Order issued by them.

E*Trade

2008 - US\$1mio⁷³

Agency: SEC

E*Trade Clearing LLC and E*Trade Securities LLC (E*Trade) are wholly owned subsidiaries of E*Trade Financial Corporation, a Delaware corporation headquartered in New York. They are broker-dealers registered with the SEC. On July 31, 2008, the SEC published an order imposing remedial sanctions, penalties and a cease-and-desist order under the Securities Exchange Act of 1934. Each of the LLCs was ordered to pay US\$500k to the US Treasury within 30 days. In the Findings portion of the Order, the SEC stated that from October 2003 until June 2005, E*Trade failed to follow its own CIP and SEC regulations. Specifically, E*Trade failed to verify the identities of secondary accountholders in newly opened joint accounts. The SEC found E*Trade's failure to be systemic, due to a lack of a cohesive

organisational structure, the lack of adequate management oversight, and miscommunications between personnel in E*Trade business groups. When using a third party vendor for vetting new customer information, E*Trade failed to forward the names of secondary accountholders to the process, in spite of its own policies to the contrary, and in spite of internal reports to internal compliance officers that the second names were not being vetted. E*Trade was directed to engage an independent consultant to assess the adequacy of E*Trade's CIP policies and procedures and whether E*Trade is in substantial compliance with both its statutory obligations and the companies' own policies and procedures.

United Bank for Africa

2008 - US\$15mio (concurrent CMPs) (plus 2007 US\$500,000 fine and CMP)⁷⁴⁻⁷⁸

Agencies: FinCEN CMP & OCC C&D and CMP

UBA is headquartered in Lagos, Nigeria. In April 2008, the OCC and FinCEN issued orders for concurrent US\$15mio Civil Money Penalties (to be satisfied by a single US\$15mio payment) in connection with the OCC's February 2008 C&D order for violations of the Bank Secrecy Act (BSA).

In the joint press release announcing the orders, then FinCEN Director James J. Freis, Jr., said, "A financial institution that recklessly disregards its obligations under the Bank Secrecy Act and continues to operate without an effective anti-money laundering programme, despite repeated warnings and a business focus on areas of recognised high risk, should expect to be penalized. The severity of this joint enforcement action is reflective of just such conduct. This is not a case of interpretation of technical issues or about minor lapses in compliance." In January 2007, due to BSA programme deficiencies, the OCC issued a Cease & Desist Order (C&D), (and fined US\$500,000), by consent, to the bank. During an OCC targeted examination conducted in November 2007 to determine compliance with the 2007 C&D, OCC examiners determined that the bank had failed to comply with the terms of the C&D and that significant BSA programme deficiencies remained pervasive and systemic, including internal control and audit deficiencies, as well as the bank's continued failure to identify and report suspicious activities.

As a result of its examination findings, the OCC issued a second Cease and Desist Order, by consent, to the bank in February 2008. It required the bank to, among other things: cease and desist from processing wire transfers, dollar drafts, and pouch transactions; retain the services of a qualified, independent consultant to conduct a fourteen-month review (from January 1, 2007 through February 29, 2008) of the bank's wire transfer and dollar draft activities to ascertain the existence of any unusual or suspicious transactions

during this period; revise and implement the bank's written programme establishing a system of internal controls and processes; and to take other needed steps to ensure compliance with suspicious activity reporting requirements.

The OCC assessed the bank a US\$15mio civil money penalty and imposed a new C&D Order as a direct result of the bank's failure to comply with the OCC's 2007 C&D and the bank's failure to correct these BSA programme deficiencies. In assessing a US\$15mio civil money penalty, FinCEN determined that the bank failed to implement an adequate anti-money laundering programme reasonably designed to identify and report transactions that exhibited indicia of money laundering or other suspicious activity involving approximately US\$197mio in suspicious transactions.

Sigue Corporation

2008 - US\$12mio CMP; US\$15mio forfeiture^{79/80}

Agencies: FinCEN and DoJ DPA

Sigue Corporation and Sigue, LLC ("Sigue") operate a money services business headquartered in San Fernando, CA, with over 7,000 agent businesses throughout the country. Sigue agreed to the issuance of a US\$12mio CMP by FinCEN for violations of BSA. In addition, Sigue entered a deferred-prosecution agreement with the Justice Department on charges of failing to maintain an effective AML programme, and agreed to forfeit US\$15mio (payment of which will satisfy the FinCEN penalty).

According to the CMP Order, Sigue "failed to implement effective internal controls, designate compliance personnel and conduct effective independent testing and training to ensure compliance with the Bank Secrecy Act." After suspecting Sigue's compliance with US money laundering prevention laws were cursorily, the US government sent undercover investigators to a number of Sigue's delegates' businesses across the country in a government sting codenamed "Operation High Wire."

Undercover agents approached Sigue Corp delegates clearly stating that the currency they wanted to send was proceeds of drug trafficking and was being sent as payment to the "source of supply." The undercover agents informed the Sigue Corp delegates that they did not want law enforcement to learn of the transactions, and that they preferred not to provide any form of identification or address information.

When Sigue Corp delegates requested some form of identification from the undercover agents, the agents produced multiple forms of identification cards, all in different names and bearing obviously different likenesses. While many delegates turned the undercover agents away, at least 59 delegates in 22 states did not, with these

59 willingly helping the investigators structure transfers to avoid currency reporting requirements, suggesting the undercover agents use admittedly false names and generally facilitating what they believed to be an effort to move drug money to Mexico. The result was that a total of US\$500,000 was moved in these sting transactions to a group of seven individuals in Mexico City.

Subsequently it would emerge in the later prosecution of Sigue Corp that from 2003 to 2005, more than US\$24.7mio in suspicious transactions were conducted through Sigue Corp agents, including those conducted by undercover US law enforcement agents. Whilst Sigue Corp had filed some SARs, particularly SARs identifying structuring, the US authorities prosecuted Sigue for the willingness of some Sigue Corp delegates to facilitate the sting transactions and for the weaknesses in the oversight and surveillance of activity undertaken by Sigue Corp delegates.

As part of the settlement with the government, Sigue agreed that it would implement and maintain a transaction monitoring system for the purpose of performing risk-based trend analysis related to sender, beneficiary, originating authorized delegate, and paying location transactional activity, setting a new benchmark in level expected for compliance with AML rules for MSBs.

The Bank of Tokyo-Mitsubishi UFJ

2008 - 1.2 mio yuan (US\$190,000)⁸¹

Agency: People's Bank of China

In 2008 as Beijing came under mounting foreign pressure to curb money laundering, it was revealed that the central bank fined the Shenzhen branch of one of Japan's biggest lenders 1.2mio yuan for failing to report suspicious transactions.

The Bank of Tokyo-Mitsubishi UFJ was among 600 financial institutions fined a total of 56.3mio yuan by the People's Bank of China for money laundering violations in 2008. The central bank's centre for monitoring and analysing suspected money laundering said it reviewed suspect transactions worth about US\$10.8bio China Business News reported, citing official statistics.

No further details of the Japanese bank's business or the transactions were given. The report did not give the names of any other financial institutions required to pay fines.

Special Focus 11 Winterflood

2008 - £4mio CMP^{82/83}

Agency: UK FSA

The FSA fined Winterflood £4mio in 2008, one of the UK's biggest fines ever handed out, after it found that the firm (part of investment bank Close Brothers) and two of its traders, Stephen Sotiriou and Jason Robins, had "engaged in market abuse" in relation to a share ramping scheme involving Fundamental-E Investments, a computer screen company. Winterflood was a market-maker in FEI and executed many trades including orders from SP Bell, a now defunct stock-brokering firm controlled by Simon Eagle, a former commodities trader.

The Winterflood case was an important one because it tested the UK's unusually broad definition of market abuse and highlighted how one firm can be held responsible for another firm's market abuse even though that firm had no actual knowledge or intent. Unlike US insider trading laws, the UK market abuse rules say they can be violated unintentionally.

The Court of Appeal's judgment in 2010 in the FSA's favour supports the broader definition and in doing so dismissed Winterflood's appeal regarding its failure to spot share ramping.

Winterflood was accused of failing to notice warning signs or querying particular trades in FEI in 2004. However, there was no allegation by the FSA that Winterflood or the traders deliberately committed an offence. In a separate action, it was established that Simon Eagle and SP Bell had "embarked on a share ramping scheme, the effect of which was to inflate the price of FEI shares". The court however found that, "Accordingly the involvement of Winterflood, Mr Sotiriou and Mr Robins was critical to the success of the share ramping scheme."

Société Générale

2008: €4mio (US\$6.3mio)⁸⁴

Agency: French Banking Regulator

French regulators fined Société Générale about €4mio (US\$6.3mio) for "grave deficiencies" in the bank's internal controls that led to a €4.9billion loss, caused by rogue trader, Jerome Kerviel. The regulatory statement said: "The weaknesses brought to light, in particular the deficiencies in hierarchical controls, carried on over a long period, throughout 2007, without being detected

or rectified by the internal control systems." It also said that Société Générale's IT systems contained "significant weaknesses" and highlighted the lack of a gross trading limit for *Kerviel*. But the regulator did say that the bank had been swift to attempt to correct these problems once they were revealed. An internal investigation at Société Générale stated that *Kerviel* bypassed risk controls at the bank to build up a trading position worth €49billion - more than the bank's own stock market value. Following the scandal, Daniel Bouton, Société Générale's Executive Chairman, split his position, transferring some of his powers to Frederic Oudea. Jean-Pierre Mustier, the head of the bank's Investment Banking unit, was also replaced.

Special Focus 12 Aon Limited

2009 - £5.25mio^{85/86}

Agency: UK FSA

Aon Limited (Aon) was fined £5.25m by the Financial Services Authority in 2009 for failing to take reasonable care to establish and maintain effective systems and controls to counter the risks of bribery and corruption associated with making payments to overseas firms and individuals. Between 14 January 2005 and 30 September 2007, Aon Ltd failed to properly assess the risks involved in its dealings with overseas firms and individuals who helped it win business and failed to implement effective controls to mitigate those risks. As a result of Aon's weak control environment, the firm made various suspicious payments, amounting to approximately US\$7mio, to a number of overseas firms and individuals.

Whilst no bribery or corruption acts could be proved, the lack of documenting the due diligence undertaken was felt sufficient by the FSA to raise a case against Aon for failing to adhere to the FSA handbook's provision on systems and controls. It can also be supposed the FSA thought that bribes probably had though been paid. In addition, under the FCPA, companies can be found guilty of not maintaining adequate books and records. There is a similar requirement in the Companies Act 2006 in the UK. Margaret Cole, then Director of Enforcement, said, "This is the largest financial crime related fine imposed by the FSA to date. It sends a clear message to the UK financial services industry that it is completely unacceptable for firms to conduct business overseas without having in place appropriate anti-bribery and corruption systems and controls."

Doha Bank

2009 - US\$5mio⁸⁷⁻⁸⁹

Agencies: FinCEN CMP and OCC C&D and CMP

In April 2009, the New York Branch of Doha Bank,

headquartered in Doha, Qatar, was assessed civil money penalties of US\$5mio by both the OCC and FinCEN, for past violations of the BSA. The two US\$5mio assessments were satisfied by a single US\$5mio payment to the US Treasury.

This action was preceded by an OCC C&D order in September 2006, in which Doha was ordered to complete a look-back of wire transfers, demand drafts and pouch items covering the period from May 1, 2004 through January 16, 2007. That review was completed in January 2008.

According to a press release from FinCEN and the OCC, "the OCC based its assessment of a US\$5mio civil money penalty, and the issuance of the C&D Order, on the Branch's failure to maintain a compliance programme reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements of the BSA, and other related BSA compliance violations. Specifically, the Branch did not adequately identify, research, report, and monitor suspicious activities occurring through the Branch's funds transfers, pouch activity, demand draft services, and correspondent relationships, and did not adequately audit and independently test such activities. The Branch also failed to conduct sufficient due diligence on its foreign correspondents. The look-back mandated by the C&D Order confirmed the BSA programme deficiencies cited in the C&D Order." FinCEN's reasons for assessing its penalty were essentially identical. More telling was then FinCEN Director Fries' comment: "Despite the current economic and resource challenges that many banks may face, Bank Secrecy Act (BSA) compliance efforts must not be diminished. Timely, complete, and accurate Suspicious Activity Reports (SARs) are critical tools available to law enforcement as a means to deter and detect criminal activity. Used in conjunction with additional financial intelligence, SARs help law enforcement to ferret out criminal elements and combat fraud that threatens our financial system. As such, failure to follow BSA rules deprives law enforcement of valuable information in the investigation and prosecution of crime. FinCEN continues to collaboratively ensure that all financial institutions follow BSA rules which in turn serve to protect our financial system."

E*Trade

2009 - US\$1mio Fine

Agency: FINRA⁹⁰

FINRA announced on January 2, 2009 that it imposed a US\$1mio fine against E*Trade Securities, LLC and E*Trade Clearing, LLC, collectively, for failing to establish and implement AML policies and procedures that could reasonably be expected to detect and cause the reporting of suspicious securities transactions. "FINRA found that between Jan.1, 2003 and May 31, 2007, E*Trade did not have an adequate AML programme based upon its business

model. Because E*Trade did not have separate and distinct monitoring procedures for suspicious trading activity in the absence of money movement, its AML policies and procedures could not reasonably be expected to detect and cause the reporting of suspicious securities transactions. The firm relied on its analysts and other employees to manually monitor for and detect suspicious trading activity without providing them with sufficient automated tools. FINRA determined that this approach to suspicious activity detection was unreasonable given E*Trade's business model."

This penalty by the non-governmental regulator of securities firms is in addition to penalties imposed earlier by the SEC in July 2008 (see case above).

Special Focus 13 Credit Suisse

2009 - US\$536mio forfeiture^{91/92}

Agencies: DoJ, OFAC, DPA

Credit Suisse paid a US\$536mio fine to US authorities for processing hundreds of millions of payments through US banks in violation of US sanctions regulations. Two of the organisations that Credit Suisse facilitated transactions for were the Atomic Energy Organisation of Iran and the Aerospace Industries Organisation, both of which are designated as proliferators of weapons of mass destruction by the US Office of Foreign Assets Control.

Credit Suisse began helping customers evade sanctions in 1986 when US sanctions against Libya were imposed. It instituted an internal policy that payment orders of Libyan banks and government agencies destined to or through the US were to be executed without stating the name of the ordering party. By 1994, Credit Suisse issued an internal instruction that the phrase "by order of a client" could be used in place of the ordering party. In 1995, after the US imposed sanctions against Iran, Iranian banks requested that Credit Suisse omit their names and Bank Identification Codes from payment messages headed for US correspondent banks. Until 2004, Credit Suisse's use of "order of a customer" was a standard procedure for processing bank payment messages involving Iranian customers. Another approach was to populate transaction party fields with "Credit Suisse" or its BIC code.

Another Credit Suisse method of hiding references to sanctioned parties in payments destined for the US was the use of abbreviations. A 2003 internal email from Credit Suisse's Iran Desk stated:

[Entry to their account works when account number plus

[XXX] is stipulated as beneficiary. What is also important of course is that applicant give details of final beneficiary as reference for the beneficiary, then it should work.

Also in 2004, Credit Suisse opened a US\$ account for a client in the name of an abbreviation (first letter of each word constituting the bank's name).

Credit Suisse used its stripping procedures to market itself to sanctioned clients. The factual statement accompanying the DPA gives the following excerpt from Credit Suisse's marketing communications:

[I]t is absolutely impossible that one of your payment instructions will be effected without having it checked in advance by our specially designated payment team at Credit Suisse in Zurich.

When Credit Suisse outsourced its US dollar clearing activities to Bank of New York, Credit Suisse notified its Iranian clients and gave them a pamphlet entitled, "How to transfer USD payments" which contained instructions for formatting payments to evade US filters.

In a 1998 letter to an Iranian customer, explaining the transfer of its US dollar clearing services to Bank of New York, Credit Suisse wrote:

"In order to provide your esteemed institution with our clearing services in US\$, we have introduced a procedure to facilitate your US\$ payments through our clearing system. The change of our USD-clearer to Ban[k] of New York, New York, will not affect our mutual relationship on any clearing transaction in US Dollars as long as the established procedure will be followed."

Credit Suisse's payment system had warnings connected to client files: "Do not mention the name of the Iranian bank in payment orders."

The payment system warnings were replaced with instructions to use the MT202 message format as a cover for the underlying transfer. Because the MT202 format used for cover payments lacked space for information about the remitter, it was necessarily left off the message and the message could not be stopped by US filters.

Credit Suisse's use of cover payments to hide the identity of sanctioned clients began in 1995 in response to a client request. An Iranian bank client requested that Credit Suisse process all of its payments using an MT202 message format to hide the bank's identity. Credit Suisse stopped using MT 103 messages for Iranian customer's transfers and instead used the MT 202. According to the DPA Factual Statement, between March 2004 and November 2005, nearly

96% of customer payment messages relating to Iranian customers were made using cover payments. However, for non-sanctioned payment messages, a mere 60% were made using cover payments.

In August 2004, a proposed merger between Credit Suisse and CSFB prompted an examination into these practices. In 2005, Credit Suisse decided to discontinue business with US-sanctioned countries, with some private banking exceptions. The institution created a new sanctions compliance framework in 2006, cooperating with US authorities investigation.

Special Focus 14 Lloyds Banking Group

2009 - US\$ 350mio⁹³⁻⁹⁵

Agencies: DoJ DPA, NYDA

Lloyds is a UK financial institution with banking operations around the world, including two offices in the US. From the mid-1990's to January 2007, Lloyds employees assisted clients in evading US sanctions by engaging in a practice called "stripping".

This involved the removal of data from payment messages to avoid the transaction filters used by US depository institutions to detect transactions involving sanctioned parties. This practice caused Lloyds' US correspondent banks to process transactions that those banks otherwise could have stopped, blocked and reported in accordance with US sanctions regulations.

In 1995, in response to US sanctions against Iran, Lloyds' UK-based unit created a procedure to manually review messages from UK-based Iranian bank clients. These clients included Banks Sepah, Melli, Tejarat, Saderat and the Iranian Overseas Investment Bank. The review was to ensure references to Iran were removed before the messages were sent to or through the US.

An internal memorandum set forth the steps. First, a payment team member would remove the payment instruction so that it could be manually processed. Second, the payment instruction would be printed out. Third, the payment team would mark up the printed payment instruction to show what information should be changed, including crossing out references to Iranian banks. Fourth, the edited message would be returned to the repairers who would type the corrected information back into the system. The resulting message would give US banks no indication that an Iranian party was involved.

In 2002, Lloyds' UK payment unit raised concerns that this practice might violate US law. Lloyds business managers argued for the practice to continue, believing that the UK payment unit was operating outside of US jurisdiction. Lloyds decided to remove some risk by moving the responsibility for stripping from its payment unit to the clients. Lloyds representatives met with UK Iranian bank clients to instruct them on how to format, themselves, payment messages to avoid detection by US OFAC filters. Lloyds employees counseled these banks not to leave payment message fields blank, but to populate the originating bank fields with special characters, which prevented the system from populating the field with the originating bank name. Lloyds employees continued to manually strip payments caught in their filters.

In 2003, the issue of "stripping" was brought to the attention of Lloyds' Group Executive Committee, which decided to stop US\$ clearing for UK Iranian banks. Between 2002 and 2004, Lloyds had processed approximately US\$300mio for UK Iranian banks via US institutions or their branches, and another US\$20mio on behalf of Libyan customers by the time sanctions against Libya were lifted in 2004. However, Lloyds continued providing these services to Sudanese bank clients until 2007, processing more than US\$20mio on behalf of Sudanese bank customers between 2002 and 2007.

In 2007, US prosecutors informed Lloyds of their investigation of its stripping practices. The case against Lloyds grew out of an investigation into how money transfers through the American banking system might have been used to finance Iran's nuclear and missile programmes. The US investigation into potential sanctions violations would expand to involve nine European banks.

On 9 January 2009, Lloyds entered into a Deferred Prosecution Agreement with the New York County District Attorney's Office and the US Department of Justice, agreeing to pay US\$350mio and criminal charges that it had caused US depository institutions to process payments in violation of US sanctions regulations. In the DPA, US authorities charged that by formatting and stripping payments to evade US filters, Lloyds caused US institutions to process transactions in violation of US sanctions regulations.

Special Focus 15 Stanford Bank

2009 - Closure⁹⁶⁻⁹⁸

Agencies: SEC, FBI, DoJ

Allen Stanford a prominent former financier and cricket mogul, is currently serving prison time in the US after having been convicted on charges that his investment company was a fraudulent Ponzi scheme. Stanford was the Chairman of the now defunct Stanford Financial Group, which included companies in the Americas and the Caribbean.

Stanford became the subject of several fraud investigations, and on February 17, 2009, he was charged by the Securities and Exchange Commission (SEC) with fraud and multiple violations of US securities laws for his alleged fraudulent activities involving US\$8bio in certificates of deposits (CDs). The FBI raided three of Stanford's offices in the US, and on February 27, 2009, the SEC amended its complaint to describe Stanford's fraudulent activity as a Ponzi scheme. On March 6, 2012, Stanford was convicted on all charges, except single count of wire fraud for allegedly bribing an Antiguan regulator with US\$9,000 Super Bowl tickets.

In early February 2009, the SEC, the FBI, the Florida Office of Financial Regulation, and the Financial Industry Regulatory Authority (FINRA) launched an investigation of Stanford Financial Group, questioning the consistently higher-than-market returns that Stanford International Bank claimed to provide its depositors. SEC officials learned that Stanford presented hypothetical investment results as actual historical data in sales pitches to clients, and that he claimed that his CDs were as safe as, or safer than, US government-insured accounts.

A leaked cable from the US Embassy in the Bahamas in 2006 reported that companies under Stanford's control were thought to be engaging in bribery, money laundering, and political manipulation. As a result, when federal agents raided the offices of Stanford Financial in February 2009, they treated it as the equivalent of a crime scene and cautioned people not to leave fingerprints.

At the request of the SEC, on February 19, 2009, FBI agents located Stanford and served him with legal papers filed by the SEC. Stanford was not arrested until a month later. The SEC charged Stanford with fraud that

was centred on an US\$8bio investment scheme. They alleged that Stanford and his accomplices operated a Ponzi scheme, in which they misappropriated billions of dollars of investors' money and falsified the Stanford International Bank's record to cover up their fraud. Stanford denied any wrongdoing. He argued that his companies had been well-run until the SEC began investigating them. Stanford's assets, along with those of his companies, were frozen and placed into receivership by a US federal judge. The judge also required that Stanford surrender his passport.

Following the allegations, various governments took over Stanford's business operations. The Eastern Caribbean Central Bank (ECCB) took over the local operations of the Bank of Antigua, which was renamed the Eastern Caribbean Amalgamated Bank. The Venezuelan government took over Stanford Bank Venezuela, the Venezuelan branch of Stanford's bank. Stanford pleaded not guilty to charges of fraud, conspiracy, and obstruction.

Stanford's trial date was set for June 25, 2009, but this was delayed due to his poor health. In February 2011, Stanford issued a US\$7.2bio counter-claim against the FBI and the SEC. In May 2011, prosecutors dropped seven charges against Stanford, leaving 14 charges outstanding, including counts of fraud, money laundering, and obstructing an SEC investigation.

Stanford's trial began on 24 January 2012. Prosecutors claimed that Stanford stole billions of dollars from investors to fund his lavish lifestyle and held his customers' money in bank accounts in Switzerland, Canada, and the UK for his own use. Another account, the "Baby Mama Trust," was held in the Cook Islands, and it included proceeds from the sale of properties tied to one of Stanford's girlfriends who bore his children.

Prosecutors claim that Stanford used customer money to purchase these properties. Stanford has also been accused of misleading investors in marketing brochures by promising that their money would be invested in easy-to-trade assets, such as stocks and bonds, when instead, he used the money to buy two Caribbean newspapers, islands, and airplanes.

Stanford was ultimately convicted on 6 March 2012 by the jury as the leader of a Ponzi scheme worth US\$7bio operated through his Antiguan-based bank. He was sentenced in June 2012 to 110 years in federal prison. James M. Davis, the former Chief Financial Officer of Stanford Financial Group, pled guilty to charges of fraud and obstruction of Justice in August 2009 and testified against Stanford. On 22 January 2013,

Davis was sentenced to five years in jail, three years of supervised release and had a judgement of US\$1bio placed against him.

The jury ruled that Stanford should forfeit US\$330mio held in offshore accounts in order to fund payments to the thousands of victims of the Ponzi scheme. The court-appointed receiver for Stanford's businesses set aside US\$80mio for victims out of the US\$216mio collected from settlements and sales of his yachts and real estate.

In order to increase the victims' recovery, the receiver has sued the Libyan government, Stanford brokers, and others who took money out of the company

Furthermore, three former Stanford employees were tried and convicted for their roles in Stanford's Ponzi scheme. Laura Pendergest-Holt, Stanford's former Chief Investment Officer, pled guilty on June 2012 to obstructing the SEC investigation into Stanford International Bank. On 13 September 2012, Holt was sentenced to three years in prison, followed by three years of supervised probation. Stanford's ex-Chief Accounting Officer Gilbert Lopez, and former Global Controller Mark Kuhrt, were each found guilty in November 2012 of 9 of 10 wire fraud counts and one count of conspiracy to commit wire fraud. The men were sentenced to prison terms of 20 years when they were sentenced in February 2013.

A former Antiguan regulator, Leroy King, has also been charged for allegedly accepting bribes from Stanford to interfere with an SEC investigation, and in April 2012 filed his fourth appeal to bar his extradition to the US.

In addition to the fraud charges against Stanford, the US Court of Appeals for the Fifth Circuit, which affirmed most of a US Tax Court's ruling, determined that Stanford's wife under-reported their 1990 federal taxes by nearly US\$500,000.

It has also been suggested that Stanford may owe hundreds of millions of dollars in federal taxes. There are four federal tax liens from 2007 and 2008 against Stanford, which amount to more than US\$212mio.

Finally, the FBI and other agencies have been conducting an ongoing investigation of Stanford since 2008 for possible involvement in money laundering for Mexico's Gulf Cartel.

Special Focus 16 UBS

2009: US\$780mio CMP⁹⁹⁻¹⁰¹

Agencies: US DoJ DPA. IRS

In 2009 UBS entered into a Deferred Prosecution Agreement with the US Government avoiding indictment on criminal charges of aiding tax evasion. The Agreement entailed UBS paying US\$780mio in fines and initially turning over the names of about 250 US clients. The Swiss parliament later voted to approve a deal between the Department of Justice and UBS in which UBS agreed to turn over the names of 4,450 US citizens who held bank accounts at UBS. Under the DPA, UBS also agreed to exit the business of providing banking services to US clients with undeclared accounts. The case arose when Bradley Birkenfeld, a private banker who formerly worked for UBS, in Geneva Switzerland provided information to the US Government about his dealings with US clients located in the US, suspected of placing money offshore to evade US taxes.

Birkenfeld sought to benefit from the IRS's Whistleblower Reward Programme, from which he would ultimately benefit, but the case as was handled by the US Justice Department took the view that the IRS programme did not provide immunity from prosecution for criminal acts and Birkenfeld was charged and pleaded guilty in 2008 being convicted on fraud conspiracy grounds and sentenced in 2009 to 40 months in jail.

In 2012, whilst the IRS awarded Birkenfeld a reward of US\$140mio, he remained incarcerated.

The case against UBS went back to 2000, when Foreign Banks who entered into an agreement with the US IRS, called the QI Programme (Qualified Intermediary) then became obliged to report to the IRS income and other information for its US clients who held US securities in a UBS account, in order to enforce increased tax compliance by US citizens with offshore accounts. It was alleged that some employees and managers within UBS helped some US citizens to open new UBS accounts inserting for example a corporate vehicle or similar in between the individual and the bank account so that the US Citizen would not be identified as a beneficiary when reporting to the IRS was required by the Bank, effectively assisting those US citizens in evading these new reporting requirements, who in turn regularly filed false tax returns which omitted the

income earned on their Swiss bank accounts and failed to disclose the existence of those accounts to the IRS.

Further information about the US client private banking cross border business was also revealed in the investigation with allegations that UBS bankers routinely traveled to the US both prospecting for new clients and meeting existing clients. It was asserted that in 2004 alone, UBS bankers traveled to the US approximately 3,800 times to discuss their clients' Swiss bank accounts.

Whilst UBS admitted making mistakes it quickly co operated with the US investigation and provided crucial information and remediated the problems, sacking managers and introducing state of the art measures to control its broader cross border business.

In 2008, ex UBS Head of Wealth Management Raoul Weil was indicted and charged with conspiring to defraud the US for his alleged role in overseeing the US cross-border business. Declared a fugitive from US justice, he has since been arrested in Italy and extradited to the US.

ANZ (Australia and New Zealand Banking Group Ltd)

2009 – US\$5.75mio¹⁰²

Agency: OFAC

In August 2009, OFAC reached a settlement with Australia and New Zealand Banking Group, Ltd. (ANZ) over trade finance transactions subject to US economic sanctions. ANZ paid US\$5.75mio to settle allegations of violations of the Sudanese Sanctions Regulations and the Cuban Assets Control Regulations. The international trade finance and foreign currency exchange activities at issue in the settlement occurred from 2004 to 2006 and involved ANZ's processing of transactions through US correspondent accounts. ANZ actively manipulated the SWIFT messages related to the Sudanese transactions by removing references to Sudan or the names of entities subject to sanctions in the US, thereby concealing the identities of the targets of US sanctions and impeding the ability of US banks to detect these violations. The settlement covers 16 transactions in the aggregate amount of approximately US\$28mio alleged to have violated the Sudanese Sanctions Regulations, and 15 transactions in the aggregate amount of US\$78mio alleged to have violated the Cuban Assets Control Regulations. OFAC agreed to mitigate the penalty based on three predominant factors. First, although ANZ did not voluntarily disclose the violations, ANZ cooperated in conducting an extensive review of the transactions and

brought to OFAC's attention additional transactions of which OFAC was not aware and which ANZ did voluntarily disclose. Second, ANZ promptly initiated a remedial policy. ANZ re-engineered its operating model to enhance its ability to identify and resolve operational gaps and weaknesses. ANZ agreed to continually audit its compliance model to ensure that future transactions that would be in violation of OFAC's regulations are not processed by or through US financial institutions. The Australian Prudential Regulation Authority also agreed to monitor the results of ANZ's internal review. Third, ANZ had not been subject to an OFAC enforcement action in the five years preceding the transactions at issue.

Amaranth Advisors LLC

2009: US\$7.5mio^{103/104}

Agency: CFTC

Amaranth lost US\$6.6 billion betting on the price of natural gas. The Greenwich, Connecticut-based hedge fund that once controlled half of the gas market collapsed in 2006, following disastrous bets by trader Brian Hunter. Amaranth only began trading in energy in 2002 increasing its bets from 2004 following the arrival of Mr Hunter from Deutsche Bank, where he had left after being demoted and moved off the trading desk for making big bets resulting in big losses. At Amaranth his positions initially performed very well benefited heavily from Hurricane Katrina which sent gas prices higher. For 2005, Mr Hunter received a bonus of US\$113mio.

By 2006 he was trading billions of dollars worth of gas contracts and using 38% of Amaranth's available capital. He traded from a remote office in Calgary Canada, far from the firms Head office and its risk managers in Connecticut in the US. Still his trading continued to be profitable, earning the firm US\$320mio in Feb 2006 and US\$1.1bio in April before the tide turned. In May losses of US\$1.1bio were incurred, despite worst case loss estimates considered by the firm of US\$350 mio. Instead of trying to trade out of the positions, Mr Hunter instead doubled up and by the end of May 2006, 50% of the firms positions were invested in energy, holding almost as many gas contracts for January 2007 delivery as the entire American public were expected to use for that month. With rivals smelling blood and calling for increased margin to continue large trades as prices continued to go against him, the firm was forced to cut its losses and record losses of US\$6bio.

In August 2009, the company agreed to pay US\$7.5mio to end an action brought by the CFTC over price manipulation. The Hedge Fund also agreed to a

US\$77.1mio settlement by Amaranth to resolve a class action brought by traders. A fine levied by another US regulator, Federal Energy Regulatory Commission (FERC) against Hunter for US\$30mio was struck out on jurisdictional grounds. "Manipulation of natural gas futures contracts falls within the CFTC's exclusive jurisdiction," the court ruled.

Special Focus 17 Royal Bank of Scotland (former ABN Amro Bank)

2010 - US\$580mio Forfeiture - DPA (US\$80mio -

2005 / US\$500mio - 2010)¹⁰⁵⁻¹⁰⁸

Agencies: DoJ DPA, FBI

In 2004, senior management at ABN Amro ("ABN") discovered that from 1996 to 2004 some ABN offices, branches, subsidiaries and affiliates were employing ways to circumvent US sanctions filters. These groups created processes to assist clients in Libya, Sudan, Iran and Sudan to move hundreds of millions of dollars through the US financial system undetected at a time when these countries were sanctioned by the US Government.

As a service to its clients, ABN employees would alter payment messages headed to the US to evade US sanctions filters. Beginning in 1995, ABN was approached by an Iranian bank to process US dollar payments for it by cleansing the messages. External counsel had advised ABN in that year that accepting such an arrangement amounted to an evasion of the US embargo against Iran. US banks are barred from direct or indirect dealings with sanctioned parties and sanctioned countries. To comply, they use filters to screen names, addresses and text fields in electronic payment messages against sanctions lists and names of geographical locations in sanctioned countries.

Nevertheless, ABN's Dubai branch accepted the arrangement and developed stripping into a routine practice. The employees instructed sanctioned entities to use code words such as "spare" in their payment messages as a signal for ABN to segregate the message from normal payment processing. ABN employees would then manually remove any information from the message that could trigger US filters. In some instances, employees replaced information with "ABN Amro." Local ABN payment manuals contained "special conditions" sections instructing how information should be stripped. A specific instruction from this manual stated:

Payments by order of Iranian Banks [A&D] ... maintaining accounts with ABN, Dubai are to be handled with extra care to ensure the wordings "Iran" etc. are not mentioned in the payment due to OFAC regulations.

Similar procedures were devised for processing letters of credit, US dollar cheques and traveller's cheques.

ABN also used certain payment message formats to hide references to sanctioned parties.

Upon discovering these practices in 2005, ABN conducted an internal investigation, terminated the practices and reported them to US authorities, continuing to cooperate with the US government throughout its own investigation. ABN Amro was fined US\$80mio in 2005. On 4 May 2010, ABN agreed to two criminal charges and a fine of US\$500mio in exchange for a deferred prosecution agreement (DPA) with the US government.

ABN's systematic stripping of payments was most likely supported by the belief that US sanctions requirements had no effect on foreign persons acting outside the borders of the US. ABN had a US presence, but was considered a "foreign bank" under US law. However, the US Department of Justice took a different view. One of the charges to which ABN agreed as part of the DPA alleged that ABN violated Title 18, US Code, Section 371 by conspiring to violate US sanctions regulations and defraud the US by impeding OFAC in its application and enforcement of US sanctions and embargo regulations.

On 10 May 2010, the US Department of Justice announced that the former ABN AMRO Bank, N.V. (now the Royal Bank of Scotland, N.V.) agreed to forfeit US\$500mio to the US Treasury. The bank was charged with a single count of violating the Bank Secrecy Act and one count of conspiring to defraud the US and violated the International Emergency Economic Power Act (IEEPA) and the Trading with the Enemy Act (TWEA). The IEEPA and TWEA are two of several laws underlying the sanctions administered by the US Treasury's Office of Foreign Assets Control (OFAC). The forfeiture was part of a deferred prosecution agreement, also filed on 10 May 2010.

According to court documents, the bank stripped information from funds transfer instructions and other transactions to disguise involvement of OFAC-sanctioned parties or to facilitate OFAC-prohibited transactions, and deliberately ignored its [OFAC and BSA] compliance obligations. From approximately 1995 and continuing through December 2005, certain offices, branches, affiliates and subsidiaries of ABN removed or altered names and references to sanctioned countries

from payment messages. ABN implemented procedures and a special manual queue to flag payments involving sanctioned countries so that ABN could amend any problematic text and it added instructions to payment manuals on how to process transactions with these countries in order to circumvent the laws of the US. Despite the institution of improved controls by ABN and its subsidiaries and affiliates after 2005, a limited number of additional transactions involving sanctioned countries occurred from 2006 through 2007.

ABN AMRO used similar stripping procedures when processing US dollar cheques, traveller's cheques, letters of credit and foreign exchange transactions related to sanctioned countries. ABN and the sanctioned entities knew and discussed the fact that, without such alterations, amendments and code words, the automated OFAC filters at banks in the US would likely halt the payment messages and other transactions, and, in many cases, the banks would reject or block the sanctions-related transactions and report the same to OFAC. By removing or altering material information, these payments and other transactions would pass undetected through filters at US financial institutions. This scheme allowed US sanctioned countries and entities to move hundreds of millions of dollars through the US financial system.

The BSA violations involved the failure of the New York branch of ABN to maintain adequate AML procedures and processes. According to court documents, beginning as early as January 1998 and continuing until approximately December 2005, ABN's New York branch office wilfully failed to establish an adequate AML programme. The office did not have adequate staffing, training and oversight, which permitted multiple high-risk shell companies and foreign financial institutions to use the bank to launder money through the US. More than US\$3.2bio involving shell companies and high risk transactions with foreign financial institutions flowed through ABN's New York branch. ABN also admitted it failed to maintain proper documentation regarding its customers or maintain readily available documentation about its high risk clients.

The DoJ has recommended dismissal of the criminal information filing after one year, based on the bank's remedial actions since 2005, previous penalties and consent agreements (see information on a 2005 ABN Amro penalty, earlier). The DPA was extended to December 31, 2011 to allow RBS more time to comply with the obligations and then the DPA was ended on that same date.

Special Focus 18 Wachovia Bank

2010 - US\$160mio (US\$110mio Forfeiture/CMP; US\$50mio CMP; C&D)¹⁰⁹⁻¹¹²

Agencies: FinCEN, DoJ, OC

Wachovia, founded in 1879, was the sixth-largest American bank in 2008. Facing US\$26bio in losses from subprime mortgage loans, it was acquired by San Francisco-based Wells Fargo, which dates back even further to 1852, for US\$12.7bio, creating the largest network of bank branches in the US. Not only did Wells Fargo have to clean up Wachovia's battered balance sheet but it also had to clean up Wachovia's business with Mexican money changes and improve its money laundering compliance.

In March of 2010, Wachovia agreed to a Deferred Prosecution Agreement with forfeiture (US\$110mio in identified Mexican drug monies) and penalties (US\$50mio Federal penalties) totaling US\$160mio. From May 1, 2004 - May 31, 2007, US\$373bio in wire transfers were received from the currency exchanges destined for Wachovia accounts, with more than US\$4bio of that in bulk cash.

The charge sheet against Wachovia states it was "the largest violation of the Bank Secrecy Act, an anti-money laundering law, in US history." In particular, the AML programme at Wachovia was found materially deficient in three of the four core elements required by the BSA. The bank failed to: establish and implement effective internal policies, procedures and controls; designate personnel to ensure day-to-day compliance; and implement an effective independent audit function to test programmes with respect to the BSA, particularly the suspicious activity reporting requirements. Wachovia and its executives avoided criminal prosecution in return for the US\$160mio payment and significant improvements in its AML programme within 12 months of the Agreement. At the time of the charges, Wachovia had already ended its relationships with foreign currency exchange houses in 2008 and said in a statement that it had begun adopting a more robust AML programme including hiring a new chief compliance officer and a BSA officer, as well as training employees and monitoring suspicious transactions with high-risk countries.

Wachovia had a well established Casa de Cambio client base from Mexico from the 1990s onwards inherited from First Union, which was merged into Wachovia

in 2002. Still Wachovia then expanded its Mexican Casa de Cambio business, for example, by acquiring the existing business from Union Bank of California which had ironically decided to close its own casa de cambio business after itself entering into a DPA with the US government on charges of failing to maintain an effective AML programme when US\$22mio in drug proceeds were identified as flowing through Mexican exchange-house, Ribadeo Casa de Cambio at Union Bank of California. Union Bank of California, a unit of San Francisco-based UnionBanCal, agreed to pay US\$31.6mio in fines and penalties (see above). Wachovia also hired a former UBOC manager who previously supervised the CDC accounts and he helped Wachovia's Miami branch to set up the structure of wire transfers. This increase in business with Mexican Casas de Cambio came despite known money laundering concerns, for example, in addition to the Union Bank of California DPA, the US government highlighted in 2005 nine casas that helped the Arellano Felix Drug Cartel to launder US\$120mio. In fact, the US government have been warning since 1996 that Mexican currency exchanges were laundering drug money through US banks. It also came at a time when many other US banks were exiting or placing restrictions on their business with Mexican and indeed more broadly Latin American Casas de Cambio.

Their acceptance of this type of business, knowing it to be higher risk should have raised alarm bells at Wachovia and at the very least money laundering controls should have been enhanced and commensurate with the risk. The failure to heed warnings from experienced Compliance Officers within the Organisation, both in London and in Miami was an expensive and dangerous error. One problematic Mexican Casa de Cambio was Casa de Cambio Puebla (see Cases in Part 2, Section 7) which would also feature in the later case of HSBC (see later in this section - 2012).

Wachovia admitted it did not do enough to spot illicit funds in its handling of US\$378bio for Mexican-currency-exchange houses from 2004 to 2007. Whilst it is not suggested that these hundreds of billions of dollars were the proceeds of drug trafficking, in fact according to the DPA the only monies forfeited were US\$110mio, it is nevertheless such a large sum, equaling almost the annual GDP of Mexico that the suggestion must be that a great deal more than US\$110mio was in fact laundered drug monies though how much this may be is impossible to say. In processing such large sums, Wachovia should have questioned whether the size of the business was commensurate and compatible with the legitimate activity performed by Casas de Cambio.

For example, Casas de Cambio play an important role in processing remittance payments though these funds usually are directed from the US to Mexico and according to the UN are approximately only US\$8bio per year.

Following the Wells Fargo acquisition and in public statements made, Wells Fargo invested US\$42mio over three years to improve its AML programme. The bank also stated, "We have substantially increased the caliber and number of staff in our international investigations group, and we also have significantly upgraded the monitoring software."

Financial Institutions, no matter the size, will be held accountable for allowing the laundering of illegal proceeds through the US banking system. It is imperative that banks maintain a robust AML programme and policies and procedures to identify possible illegal activity. More in depth due diligence by Wachovia would have identified the source of funds flowing through the Wachovia accounts from the Mexican currency exchanges and questioned the reason for bulk cash deposits that exceeded the customer's expected activity. Adequate AML monitoring and training would have captured numerous suspicious transactions such as round-number wire transfers on the same day for a single account and deposits of traveller's cheques with sequential numbers, that should have raised red flags. Failing to have this, however, caused Wachovia to act as a channel to launder money.

Special Focus 19 Barclays Bank

2010 – US\$298mio¹¹³⁻¹¹⁵

Agencies: DoJ DPA, OFAC, NYDA

In 2010, Barclays agreed to pay close to US\$298mio to US authorities, following allegations that it engaged in practices that prevented US banks from detecting 1,285 transactions involving Cuba, Iran, Libya, Burma and Sudan, transferring approximately US\$500mio through the US by altering payments to evade sanctions filters used by US banks. This was the first US fine of this magnitude where all of the apparent violations were voluntarily disclosed to enforcement authorities.

US authorities charged Barclays with intentionally routing payments for sanctioned parties through its own sundry accounts, disguising the originator. The use of the sundry account led Barclays' New York branch to believe that the payments was originating from Barclays.

A sundry account is a bank's internal suspense account generally used for recording miscellaneous items until an appropriate account entry is made.

Barclays created an internal process for altering payment messages that would otherwise have alerted US financial institutions about the true origins of the funds. Beginning in 1987, Barclays received a request from an Iranian bank not to mention its name on a payment message destined for the US. Barclays converted this request into a process of preparing payment messages without mentioning the name of the client.

Barclays' payment operations manual contained instructions on how to process payments for sanctioned bank clients. The manual instructed that the transfer should be formatted as a cover payment using an MT202 message with no mention of the sanctioned client. The manual also directed operations personnel to seek special routing instructions for US dollar transactions involving clients that were sanctioned by the US.

Payments stopped in Barclays' sanctions filters would either be 1) returned to the remitting bank indicating which words had to be removed from the message to bypass filters, 2) converting a serial MT103 message to a cover payment requiring an MT202 format that hid the underlying transaction parties, or 3) stripping or altering the information triggering the filter.

Most banks use a screening filter to check incoming and outgoing payments for sanctioned countries or references to sanctioned parties. Barclays' UK office employed a filter for screening only those MT202s headed for the US, and not the corresponding MT 103s that described the underlying transaction but would not be routed through the US.

Barclays deliberately used the MT202 format instead of a serial MT103 to hide the underlying transaction information. One Barclays employee explained in an email:

"[W]e can get around (OFAC seizure) by sending only cover payments to US banks and then make MT103 direct to beneficiary's bank. The MT202 cover must not mention of (sic) the offending entity which could cause funds to be seized. A good example is Cuba which the US says we shouldn't do business with but we do."

An internal memo stated in a relevant part as follows: "Changing to different message types would be much more expensive to us. Moral risk exists if we carry on using cover payments but that is what the industry does.

I[n] M[y] H[umble] O[pinion] we should carry on using cover payments and accept that there is a risk of these being used on occasion to hide true beneficiaries (who may or may not be sanctioned individuals or entities)."

This quote reflected a misguided belief that no legal risk existed so long as the transactions were initiated from outside the US.

In 2006, senior management at Barclays learned that several cover payments involving sanctioned parties had been routed through the NY branch on purpose. They made a voluntary disclosure to US authorities immediately. The US Department of Justice and the Manhattan District Attorney's Office launched an investigation into Barclays' practices that lasted almost three years.

Barclays agreed in 2010 to pay a US\$298mio fine and enter into a Deferred Prosecution Agreement with US authorities. Barclays admitted to violating New York law by falsifying the records of US banks, and to wilfully violating US sanctions laws. Barclays transferred approximately US\$500mio in transactions violating US sanctions laws from 2000 to the end of 2006.

US authorities remarked that the fine Barclays received could have been greater, had Barclays not voluntarily disclosed the transactions. Additional mitigators included Barclays' cooperation, its own extensive review of transactions between 2000 and 2007, its creation of a new, enhanced sanctions policy and its voluntary exit of relationships with banks and other entities sanctioned by the US.

Deutsche Bank

2010: US\$553.6mio fine DPA in connection with the sale of fraudulent tax shelters¹¹⁶

Agency: US DOJ

Deutsche Bank AG, Germany's largest bank, admitted criminal wrongdoing and agreed to pay US\$553.6mio to avoid prosecution in the US over fraudulent tax shelters that generated US\$29bio in "bogus" tax losses. The settlement includes a US\$149mio civil penalty, the fees that Deutsche Bank generated from the shelters, and the taxes and penalties the Internal Revenue Service was unable to collect from taxpayers because of the misconduct, according to the agreement. From 1996 to 2002, "Deutsche Bank assisted high net worth US citizens, who, through 2005, reported approximately US\$29.3bio in bogus tax benefits on their tax returns," according to the agreement. "DB acknowledges that it was wrong and unlawful to have engaged in these

transactions and regrets having done so." As part of the settlement, Deutsche agreed to the appointment of an independent expert to ensure the bank doesn't use transactions to defraud the IRS again, according to the agreement. The bank said in a statement. "Deutsche Bank is pleased that this investigation, which concerned transactions that ceased more than eight years ago, has come to a resolution." Deutsche Bank admitted that it participated in 15 different shelters, including transactions called "BLPS," "FLIP" and "HOMER," in at least 1,300 deals for over 2,100 customers. As part of the agreement, Deutsche Bank admitted that it knew or should have known that its participation in the deals was meant to create the appearance of legitimate investment activity, even though their "primary purpose" was to avoid taxes. The bank also said it knew that documents falsely describing the transactions would be used by taxpayers and promoters of the shelters.

The settlement stems from a US probe into illegal tax shelters sold by accounting firm KPMG LLP. The US previously brought criminal charges against former KPMG executives, which were eventually dismissed in 2007 after the firm paid a US\$456mio fine. In addition, HVB Group agreed to pay US\$29.6mio to avoid prosecution on charges the Munich-based bank helped KPMG sell shelters. Criminal cases were also brought against numerous executives, with 17 ex-KPMG executives originally accused, with 3 of these convicted at trial. The US crackdown on illegal tax shelters also targeted Jenkens & Gilchrist, a Dallas-based law firm that once had 600 lawyers and which shut down after agreeing to pay millions of dollars to avoid prosecution for selling these illegal tax shelters. Executives at accounting firms BDO Seidman and Ernst & Young were also convicted of selling illegal shelters to wealthy clients. The E&Y men had all been members of what E&Y originally called its "VIPER" Group (for "Value Ideas Produce Extraordinary Results") and later renamed the "Strategic Individual Solutions Group". Ernst & Young for itself agreed to pay US\$123mio and admitted to wrongful conduct by some of its partners and employees in connection with the firm's participation, from 1999 to 2004, in the promotion of abusive tax shelters to rich individuals. BDO paid US\$50mio.

Pamrapo Savings Bank

2010: US\$6mio - US\$5mio CMP satisfied by Forfeiture and US\$1mio Fincen fine and guilty plea for BSA violations¹¹⁷⁻¹¹⁹

Agencies: DoJ; FDIC; OTS and AG/NJ & Fincen

Pamrapo Savings Bank S.L.A., a wholly-owned subsidiary of Pamrapo Bancorp Inc., pleaded guilty to conspiracy to violate the Bank Secrecy Act and has

agreed to forfeit US\$5mio to the US government. It was also fined US\$1mio for BSA violations by FinCEN. According to the criminal information filed in US District Court in Trenton, N.J., Pamrapo Savings Bank conspired with others to conceal its customers' illegal or suspicious activities by failing to file currency transaction reports (CTR) and suspicious activity reports (SAR) and by wilfully failing to maintain adequate anti-money laundering programmes.

Pamrapo Savings Bank admitted that it wilfully violated the Bank Secrecy Act to avoid the expenses associated with compliance, despite federal and state banking regulators telling Pamrapo Savings Bank as early as 2004 that its Bank Secrecy Act and anti-money laundering programmes contained serious and systemic deficiencies in critical areas required under the law. Specifically, Pamrapo Savings Bank admitted during its guilty plea that it unlawfully failed to file CTRs and SARs related to approximately US\$35mio in illegal and suspicious financial transactions, including more than US\$5mio in structured currency transactions. The bank acknowledged that its wilful failure to maintain adequate Bank Secrecy Act and anti-money laundering programmes resulted in numerous and repeated violations of the law. In one specific example outlined in court documents, from approximately March 2005 to September 2006, a co-conspirator cashed approximately 586 cheques worth a total of US\$3.2mio, payable to "cash" at multiple branches of Pamrapo Savings Bank. Each cheque was under US\$10,000, thus structured to evade the bank's obligation to file CTRs. Ultimately, according to the court documents, Pamrapo Savings Bank wilfully failed to file a SAR related to these known and repeated violations of the Bank Secrecy Act. In addition, Pamrapo Savings Bank admitted that it made false and misleading statements to bank regulators to prevent regulatory oversight and enforcement of its deficient Bank Secrecy Act compliance programmes.

Special Focus 20 Goldman Sachs & GS International

**2010 - US\$591.5mio / £17.5mio, US\$550mio CMP/
Disgorgement US\$15mio¹²⁰⁻¹²³**

Agencies: FSA, SEC

Goldman Sachs Corp (GSC) agreed to pay US\$550mio and US\$15mio disgorgement to the SEC with regards to their Abacus programme. The Abacus programme refers to a synthetic collateralised debt obligation deal,

during which the SEC alleged that GSC and Fabrice Tourre made 'materially misleading statements and omissions'. The Abacus deal allowed GSC to sell short positions, but also to carry out its own shorts at the same time. Under particular scrutiny was the Abacus deal GSC constructed for John Paulson, acting on behalf of his hedge fund Paulson & Co. Inc., who approached GSC with the request that they set up a deal that allowed the hedge fund to short multiple RMBS securities. Email evidence, in particular those of Fabrice Tourre (employed on the Correlation Trading Desk), revealed that GSC was fully aware Paulson sought an investment that would perform poorly, thus allowing him to profit from the short position, at the expense of long investors. GSC's function in the deal was as an agent and administrator, taking fees for its services rather than a stake in the investment. Whilst criminal charges against Tourre failed, civil charges against him filed by the SEC succeeded and the court levied a fine of US\$825,000 against him.

On 9 September 2010, the Financial Services Authority (FSA) fined Goldman Sachs International (GSI) £17.5mio (US\$26.5mio) for its breach of FSA principles, in particular its failure to introduce systems and controls ensuring compliance with UK reporting regulations. GSI was found guilty of failing to report information relevant to the investigation launched by the US Securities Exchange Commission (SEC) into the Abacus 2007-ACI synthetic collateralised debt obligation. The Abacus product was structured by GSI's US counterpart, Goldman Sachs & Co. (GSC). As a result of the SEC investigation, GSC and Fabrice Tourre were issued Wells Notices containing allegations of serious violations of US securities law in respect to Abacus. GSI then failed to comply with FSA Principle 11, under which the FSA must be notified of any Wells Notices. In July of 2010, Margaret Cole, managing director of enforcement and financial crime, concluded that 'GSI did not set out to hide anything, but its defective systems and controls meant that the level and quality of its communications with the FSA fell far below what we expect of an authorised firm'.

Trillium Capital

2010 – US\$1mio fine, \$173,000 Disgorgement^{124/125}

Agency: FINRA

Trillium Capital, a high frequency trading firm in New York, was fined by FINRA for quote stuffing and market manipulation. The fine of US\$1mio is the first of a high frequency trading firm ever to be charged with using an illicit high frequency trading strategy. HFT firms have been suspected of manipulative practices for years, but no one has ever been able to prove anything.

FINRA alleged that Trillium, through nine proprietary traders, entered numerous layered, non-bona fide market moving orders to generate selling or buying interest in specific stocks. By entering the non-bona fide orders, often in substantial size relative to a stock's overall legitimate pending order volume, Trillium traders created a false appearance of buy or sell-side pressure. This trading strategy induced other market participants to enter orders to execute against limit orders previously entered by the Trillium traders. Once their orders were filled, the Trillium traders would then immediately cancel orders that had only been designed to create the false appearance of market activity. As a result of this improper high frequency trading strategy, Trillium's traders obtained advantageous prices that otherwise would not have been available to them on 46,000 occasions. Fines and suspensions were also handed out to the traders involved, the highest for John J Raffaele: US\$220,000 fine, US\$78,245 in disgorgement, and a two-year suspension and for the Chief Compliance Officer, Rosemarie Johnson: US\$50,000 fine, and a one-year suspension.

Royal Bank of Scotland

2010 - £5.6mio CMP¹²⁶

Agencies: UK FSA

In August 2010, the UK FSA levied one of its largest fines of £5.6mio (US\$8.5mio) to date on the RBS Group for not having controls in place between December 2007 and December 2008 for screening customers and transactions against an HM Treasury sanctions list, creating the risk of facilitating terrorist financing.

Special Focus 21 Merrill Lynch

2011 - US\$10mio penalty, C&D^{127/128}

Agency: SEC

Merrill Lynch was fined US\$10mio to settle charges brought by the SEC who accused the firm of misusing customers' order data to make trades for its own account and for failing to disclose trading fees. The firm's equity strategy desk improperly obtained details of trades the firm's institutional clients were making and placed the same trades for its own account, the SEC said. "Investors have the right to expect that their brokers won't misuse their order information," said Scott W Friestad of the SEC's Division of Enforcement. "The conduct here was clearly inappropriate. Merrill's proprietary traders had improper access to information about the firm's

customer orders, and misused it to place trades on the firm's behalf."

Between February 2003 and February 2005, Merrill operated a proprietary trading desk, known as the Equity Strategy Desk ("the ESD"), which traded securities solely for the firm's own benefit and had no role in executing customer orders. The ESD was located on Merrill's equity trading floor in New York City, where traders on Merrill's market making desk received and executed orders for Merrill's institutional customers. While Merrill represented to customers that their order information would be maintained on a strict need-to-know basis, Merrill's ESD traders obtained information about institutional customer orders from traders on the market making desk and used it to place trades on Merrill's behalf. In doing so, Merrill misused this information and acted contrary to its representations to customers.

Between 2002 and 2007, Merrill had agreements with certain institutional and high net worth customers that Merrill would charge only a commission equivalent for executing riskless principal trades. In certain instances in which Merrill had these arrangements, Merrill also charged customers, in addition to a commission equivalent, undisclosed mark-ups and mark-downs by filling customer orders at prices less favorable to the customer than the prices at which Merrill purchased or sold the securities in the market. This charging of undisclosed mark-ups and mark-downs was improper and contrary to the agreements the firm had with its customers.

Ocean Bank

2011 - US\$10.9mio CMP , \$10.9mio Forfeiture, DPA¹²⁹⁻¹³³

Agencies: FinCEN, FDIC, FL Office of Financial Regulation, DoJ

On August 22, 2011, FinCEN, the FDIC and the FL Office of Financial Regulation (OFR) issued a joint press release announcing Orders for the assessment of concurrent civil money penalties of \$10.9 million against Ocean Bank, Miami, Florida, for violations of federal and state Bank Secrecy Act (BSA) and anti-money (AML) laundering laws and regulations. Ocean Bank, without admitting or denying the allegations, consented to payment of the civil money penalties, which was satisfied by a single payment to the US Government. "The Bank failed to recognise and mitigate risks and report transaction activity often associated with money laundering involving direct foreign account relationships in high-risk jurisdictions, particularly Venezuela," noted then FinCEN Director

James H. Freis, Jr. "The Bank's failure to respond to such risk with commensurate systems and controls was both systemic and longstanding. The civil money penalties and forfeiture concludes joint investigations by FinCEN, the Drug Enforcement Administration, Internal Revenue Service-Criminal Investigation and the US Attorney's Office for the Southern District of Florida, and parallel examinations conducted by the Federal Deposit Insurance Corporation and the Florida Office of Financial Regulation."

Pacific National Bank

2011 - US\$7mio CMP¹³⁴⁻¹³⁶

Agencies: FinCEN, OCC

The OCC issued a Consent Order for a US\$7mio Civil Money Penalty against Pacific National Bank, Miami, FL. FinCEN had ordered a concurrent US\$7mio penalty (a single \$7 million payment will satisfy both penalty orders). The OCC had issued an earlier Consent Order against the bank in 2005, that the bank had failed to establish and maintain procedures reasonably designed to assure and monitor [its] compliance with the Bank Secrecy Act and that the bank had violated the OCC's SAR requirements and BSA compliance programme regulations. In an exam starting on March 25, 2009, the OCC determined that the bank continued to be in violation of the BSA and Treasury and OCC regulations. Similar violations were identified in a March 23, 2010 exam. Among the factors cited as causing the bank's failure to comply are (i) failure to recognise the risk inherent in foreign correspondent bank accounts and to adequately monitor transactions in light of that risk; (ii) inadequate staffing of the BSA department; (iii) failure to have adequate policies and procedures governing the foreign correspondent bank accounts; and (iv) inadequate collection and analysis of customer due diligence and enhanced due diligence information. In the exams, the OCC found that the bank failed to: develop and implement an effective risk assessment programme; ensure that sufficient and qualified Bank resources were available to effectively manage the BSA/anti-money laundering risk, comply with applicable laws and regulations, correct violations, and remediate other deficiencies addressed in the 2005 BSA Order in a timely manner; implement adequate policies, practices, procedures and internal controls for conducting customer due diligence and enhanced due diligence; implement effective policies, procedures, and internal controls to ensure effective monitoring, customer due diligence, and enhanced due diligence pertaining to the Bank's foreign correspondent bank accounts; implement appropriate procedures for identifying, monitoring and reporting suspicious activity; identify and report suspicious activity involving

foreign correspondent bank accounts; file suspicious activity reports and report ongoing suspicious activity in a timely manner; ensure that adequate and timely independent audits were conducted and that full audit reports issued; and identify and monitor suspicious activity in the bank's bill payment systems.

Zions First National Bank

2011 - US\$8mio CMP^{137/138}

Agencies: OCC, FinCEN

Zion's First National Bank is headquartered in Salt Lake City, Utah, with 148 offices in Utah. On February 11, 2011, the OCC and FinCEN each announced the issuance of concurrent consent orders for the assessment of US\$8mio civil money penalties. The two CMPs were satisfied by a single payment of US\$8mio. The OCC Consent Order focuses on activity of Zion's former foreign correspondent business, which was wound down in 2008. The following is excerpted from the FinCEN Order: "Zions utilised RDC to process certain deposit items from its non-US correspondent accounts. RDC, a deposit-transaction delivery system, allows a financial institution to receive digital information from deposit documents captured at remote locations such as financial institution branches, ATMs, domestic and foreign correspondents, or locations owned or controlled by commercial or retail customers of the financial institution. In substance, RDC is similar to traditional deposit-delivery systems at financial institutions. However, RDC enables customers of financial institutions to deposit items electronically from locations globally. RDC introduces additional risks beyond traditional deposit-delivery systems because it enables a bank's customers to scan a cheque or monetary instrument and then send the scanned or digitized image to the financial institution without the need for face-to-face transactions. This change in the interaction process for executing such transactions raises several challenges, including but not limited to: (i) the difficulty of determining in what jurisdiction the equipment is being used and by whom; (ii) development of internal controls to ensure transaction data and check images are not altered; and (iii) implementation of monitoring by qualified personnel for potentially fraudulent, sequentially numbered or altered money orders or traveller's cheques."

Mizrahi Tefahot Bank

2011 - US\$350,000 CMP^{139/140}

Agencies: FDIC, CA DFI

Mizrahi Tefahot Bank, Ltd. is chartered as a US branch of an Israeli foreign institution. It has one office, in Los Angeles, CA. On January 31, 2011, the FDIC and the

California Department of Financial Institutions (DFI) issued the bank a US\$350,000 CMP Order, half to be paid to the US Treasury and half to the DFI. The Order states that the agencies believe that from at least 2007 through 2009, the bank lacked an adequate programme to monitor, analyze, and report suspicious activity. In addition, the FDIC and the DFI have determined that Mizrahi failed to comply with an August 27, 2008 Consent Order issued by the FDIC and the DFI.

JP Morgan Chase Bank
2011 – US\$88.3mio fine^{141/142}

Agency: OFAC

In 2011, OFAC announced a US\$88.3mio fine against US-based JP Morgan Chase Bank, N.A (JPMC) for a collection of violations of various OFAC sanctions restrictions over a 5 and a half year period. OFAC determined that certain of JPMC's violations were egregious, including the following: failing to disclose to US authorities the fact that it processed 1,711 wire transfers involving Cuban nationals between December 12, 2005 and March 31, 2006, totaling approximately US\$178.5mio; failing to respond adequately to an OFAC administrative subpoena about its extension of a trade loan valued at US\$2.9mio to the bank issuer of a letter of credit in which the underlying transaction involved a blocked vessel connected to Iran; and failing to produce responsive documents to an OFAC administrative subpoena regarding wire transfers referencing Khartoum, Sudan. Other violations determined non-egregious by OFAC included the following: advice and confirmation of a US\$2.7mio letter of credit in which the underlying transaction involved a vessel affiliated with Iran; advice and confirmation of a US\$79,308 letter of credit involving goods destined for Sudan; and transfer of 32,000 ounces of gold bullion valued at US\$20mio to the benefit of a bank in Iran. While OFAC halved the proposed penalty of US\$178mio because of JPMC's cooperation, it also determined that JPMC recklessly failed to exercise a minimal degree of caution or care regarding its sanctions obligations. This determination was made despite the fact that JPMC had conducted investigations and made voluntary disclosures in certain cases. The aggravating factors in JPMC's case included delays in making voluntary disclosures of violations and incomplete responses to government subpoenas. JPMC's conduct did not involve systematic evasion efforts, such as "payment stripping", that formed the basis of enormous fines in years past against non-US institutions like ABN Amro, Lloyds, Credit Suisse, and Barclays. The common thread through those actions was each institution's mistaken belief that they were acting outside of US jurisdiction and beyond the risk of fines and penalties.

Deutsche Securities Korea
2011 - KRW1bio (US\$884,000)¹⁴⁴
Agency: Korea Exchange, Financial Supervisory Service

Deutsche Securities Korea was fined KRW1bio (US\$884,000) for market manipulation around the KOSPI200 stocks and derivatives trading on 11 November 2010 ("11.11 option shock"), a KOSPI200 options' expiry date. This is the highest fine by the Korea Exchange (KRX) ever imposed against a brokerage firm for market abuse and three employees involved were heavily sanctioned. According to investigation results, Deutsche sold KRW2.4424 trillion (US\$ 2.2bio) worth of stocks listed in the KOSPI200, which they had purchased through index arbitrage trading, in the last ten minutes before the market close. Due to the massive manipulative orders, KOSPI200 index plunged 2.78% and they gained illegal profit of KRW44.87bio (US\$40.5mio) from the trading. The actions have been dubbed "option terrorism".

Lebanese Commercial Bank
2011¹⁴⁵
Agency: FINCEN - US\$102 mio forfeiture

US authorities (Fincen) designated (actually proposed to designate though in effect has the same effect) Lebanese Commercial Bank (LCB) a financial institution of primary money laundering concern (under the US Paytrot Act) and froze LCB assets of US\$150mio held in the correspondent Bank of another Lebanese Bank, ultimately leading to the forfeiture of US\$102mio following an agreement reached. The US Government alleged that from approximately January 2007 to early 2011, at least US\$329mio was transferred by wire transfer from LCB and other financial institutions, primarily two Lebanese money exchange houses, to the US for the purchase of used cars that were then shipped to West Africa. Cash from the sale of the cars, along with the proceeds of narcotics trafficking, were funneled to Lebanon through Hezbollah-controlled money laundering channels. LCB played a key role in these money laundering channels and conducted business with a number of Hezbollah-related entities. Hezbollah is a US Department of State designated Foreign Terrorist Organisation, a Specially Designated Terrorist, and a Specially Designated Global Terrorist. Following the FinCEN action, another Lebanese financial institution, Société Générale de Banque au Liban acquired most of the assets of LCB. In addition, a second agreement was reached in June 2013, regarding claims against the Hassan Ayash Exchange Company ("Ayash"), one of the Lebanese money exchange houses allegedly involved in the money laundering scheme.

Under this settlement, Ayash agreed to forfeit more than US\$720,000 to the US government.

Turkish Bank (UK)
2012 - £294,000¹⁴⁶
Agency: UK FSA

The Financial Services Authority said it fined the Northern Cyprus-headquartered bank £294,000 for AML failures after a previous warning. This is only the second time that the FSA has fined a bank at that time under anti-money laundering regulations that came into force in 2007, following the £5.6mio penalty levied on the Royal Bank of Scotland in 2010 for not having tight enough controls to guard against payments from sanctioned parties (see above). Turkish Bank did not properly vet clearing and payment services offered to nine banks in Turkey and six based in Northern Cyprus between 2007 and 2010, leading to £114.5mio flowing through accounts that were insufficiently checked, the FSA said, adding that Turkish Bank did not keep proper records. UK banks are meant to undertake more stringent research on lenders based outside the European Economic Area to which they provide correspondent services. The fine follows a review of the banking sector by the FSA, when it found that about a third of the banks it studied dismissed serious allegations about customers without sufficient due diligence. This prompted the regulator to put banks on notice a year ago that it would step up its examination of their AML controls. "Turkish Bank fell far short of the standards we expect of firms in managing their money laundering risks. This was despite clear warnings from the FSA that it needed to improve," said Tracey McDermott, acting director of the agency's financial crime and enforcement division. "Turkish Bank's correspondent banking business made it particularly vulnerable to money laundering risks and its failings exposed UK financial services to the possibility that money could be laundered through the UK." Turkish Bank settled with the FSA, which lowered a fine that otherwise would have been more than £400,000. "This was a painful experience and we have now tidied up our act," Bob Long, the bank's managing director, told the Financial Times. "We were not deliberate or reckless, and no actual money laundering was detected in our subsequent review; it's simply that our procedures were not up to scratch."

Mizrahi-Tefahot Bank
2012 - NIS3.8mio (US\$974,000)¹⁴⁷
Agency: Bank of Israel

The Israeli Banking Corporations Sanctions Committee regarding the Prohibition on Money Laundering

and Terror Financing decided on September 19, 2012 to impose a financial sanction of NIS3.8mio (US\$974,000) on Mizrahi-Tefahot Bank Ltd. (Mizrahi) for infringing the banking directives on the Prohibition on Money Laundering Law, 2000. The infringements and faults are based on the findings in the report of an examination by the Banking Supervision Department carried out in 2007–10. The examination report findings indicated several infringements which led to the financial sanction. Most of the infringements derived from improper preparation by Mizrahi, primarily of the following types of issues: Management of accounts for lawyers without obtaining an appropriate declaration on the beneficiary; Failure to report unusual transactions; Deficiencies and faults in information transferred to the Israel Money Laundering and Terror Financing Prohibition Authority; Failure to take adequate actions to obtain declarations on beneficiaries in accounts opened, in accordance with the MLO. Mizrahi did not make carrying out a transaction contingent on obtaining the declaration on beneficiaries, despite the fact that the customer was in the branch; Notably late submission of reports to the Israel Money Laundering and Terror Financing Prohibition Authority. In its decision, the Committee took into account Mizrahi's actions to rectify the above faults.

Coutts & Company (RBS Group)
2012 - £8.75mio (US\$13.25mio) CMP¹⁴⁸
Agency: UK FSA

The UK Financial Services Authority (FSA) fined Coutts & Company (Coutts) £8.75mio for failing to take reasonable care to establish and maintain effective anti-money laundering (AML) systems and controls relating to high risk customers, including Politically Exposed Persons (PEPs). The failings at Coutts were serious, systemic and were allowed to persist for almost three years. They resulted in an unacceptable risk of Coutts handling the proceeds of crime. In October 2010, the FSA visited Coutts as part of its thematic review into banks' management of high money laundering risk situations. Following that visit, the FSA's investigation identified that Coutts did not apply robust controls when starting relationships with high risk customers and did not consistently apply appropriate monitoring of those high risk relationships. In addition, the FSA determined that the AML team at Coutts failed to provide an appropriate level of scrutiny and challenge. The FSA identified deficiencies in nearly three quarters of the PEP and high risk customer files reviewed. Tracey McDermott, acting director of enforcement and financial crime, said: "Coutts' failings were significant, widespread and unacceptable. Its conduct fell well below the standards we expect and the size of the financial penalty demonstrates how seriously we view its failures. "Coutts was expanding its customer base which in-

creased the number of high risk customer relationships. The regulatory environment in relation to financial crime had also changed. It is therefore particularly disappointing that Coutts failed to take appropriate steps to manage its AML risks. This penalty should serve as a warning to other firms that, not only should they ensure they constantly review and adapt their controls to changing financial crime risks within their businesses, but that they must also make changes to reflect changing regulatory or other legal standards.¹⁵³ As a result of the FSA's review, a number of improvements and recommendations have already been, or are being, implemented. These include significant remedial amendments to PEP and other high risk customer files to ensure that appropriate due diligence information about Coutts' customers has been assessed and recorded. Coutts agreed to settle at an early stage and therefore qualified for a 30% discount. Were it not for this discount, the FSA would have imposed a financial penalty of £12.5mio. Specifically, in one or more of each inadequate file Coutts failed to: gather sufficient information to establish the source of wealth and source of funds of its prospective PEP and other high risk customers; identify and/or assess adverse intelligence about prospective and existing high risk customers properly and take appropriate steps in relation to such intelligence; keep the information held on its existing PEP and other high risk customers up-to-date; and scrutinise transactions made through PEP and other high risk customer accounts appropriately.

Habib Bank

2012 - £525,000 CMP¹⁴⁹

Agency - UK FSA

Habib Bank, a Swiss bank of Pakistani parentage was fined by the UK FSA £525,000 alongside its former money laundering reporting officer Syed Itrat Hussain who was fined £17,500 for failures in setting up adequate AML systems and controls. The failings at Habib happened between 2007 and 2010, and exposed the firm to an "unacceptable risk" of money laundering. The FSA says Habib failed to set up and maintain adequate controls for assessing the level of money laundering risk posed by its customers. Habib maintained a high risk country list but this excluded certain high risk countries on the basis that it had group offices in them. The bank also failed to carry out appropriate due diligence on higher risk customers. In two-thirds of the 68 customer files it reviewed, the FSA found instances where the account had been inappropriately classified as normal risk, insufficient information or supporting evidence had been gathered, and/or enhanced due diligence had not been carried out ahead of transactions on the account. FSA acting director of enforcement and financial crime Tracey McDermott says: "Habib's failings were unacceptable. Habib's belief that local knowledge of a country through a group office mitigated the higher money laundering risk posed by that country was entirely misconceived. "It is critical that money laundering

reporting officers properly evaluate, on an ongoing basis, the adequacy and effectiveness of the anti-money laundering systems and controls which they are responsible for. Where individuals fail to meet their regulatory responsibilities we will not hesitate to take action."

Special Focus 22

HSBC

2012 - US\$1.96bio - US\$1.256bio Forfeiture (incl US\$375 to OFAC) / DPA, \$US665 civil penalties (US\$500mio to OCC; US\$165mio to FED)/ US\$41.8mio by Mexican Regulators¹⁵⁰⁻¹⁵⁴

Agencies: DoJ, OFAC, OCC, Fed, FinCEN, DANY

In December 2012, HSBC Bank USA, N.A. (HSBC US) and HSBC Holdings plc (together, HSBC) agreed to forfeit US\$1.256bio and enter into a Deferred Prosecution Agreement with the Justice Department for HSBC's violations of the Bank Secrecy Act (BSA), the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA). According to court documents, HSBC US violated the BSA by failing to maintain an effective AML programme and not conducting appropriate due diligence on various foreign account holders. The HSBC Group violated IEEPA and TWEA by illegally conducting transactions on behalf of customers in Cuba, Iran, Libya, Sudan and Burma – all countries that were subject to sanctions enforced by the Office of Foreign Assets Control (OFAC) at the time of the transactions. HSBC's DPA recognised the extensive remedial actions taken by HSBC and HSBC's agreement to continue to enhance its AML programmes and OFAC compliance. These actions included: 1) Resource Investment; 2) Organisation of AML Compliance Department; 3) Global Compliance Standards; 4) Global Responsibility for the Head of HSBC Group Compliance; 5) Global Risk Management; 6) Bonus Structure; 7) Termination of Risky Business; 8) Training and Procedures for Timely Notification of Red Flags; and 9) Due Diligence Requirements. Noteworthy among these provisions is the substantial compliance remediation efforts that HSBC performed prior to entering the DPA, including nearly ten-fold increases in compliance spending and staffing, exiting more than 100 business relationships for risk reasons, and undertaking a comprehensive overhaul of its compliance structure, controls, and procedures.

Furthermore it was announced that: Spending by HSBC Bank USA on staff allocated to AML compliance increased approximately nine-fold even before the entry of the DPA, and the Bank increased its number

of AML compliance staffing nearly ten-fold. The Bank also adopted a new automated monitoring system that monitors every wire transaction moving through the institution; HSBC Bank USA strengthened the compliance department's reporting lines and elevated its status within the Bank by (i) separating the Legal and Compliance departments, (ii) requiring that the AML compliance director report directly to the Chief Compliance Officer, and (iii) providing that the AML compliance director report directly to the Board and senior management about the status of the Bank's BSA and AML compliance programme on a regular basis; HSBC Group's remedial measures included adoption and implementation of global compliance standards, including applying the highest or most effective AML requirements for operations worldwide, and using OFAC's and other sanctions lists to conduct screening in all jurisdictions and in all currencies; HSBC Group centralized oversight of every compliance officer worldwide to ensure that both accountability and escalation flow directly to and from HSBC Group Compliance; the agreement identified a number of measures with regard to risk management, including implementing a new customer risk-rating methodology and the adoption of risk guidelines for considering business opportunities "in countries posing a particularly high corruption/rule of law risk" and limiting business in countries where there is a high risk of financial crime; HSBC Group changed its bonus structure for its senior executives to consider executives' fulfillment of its compliance standards and values; HSBC Bank USA terminated certain business relationships and exited the Banknote business, and HSBC Group sold subsidiaries and withdrew from nine countries by applying "a more consistent global risk appetite"; the agreement requires HSBC to implement specific procedures and training to ensure the compliance officers responsible for sanctions are promptly made aware of requests or attempts to withhold or change identifying information that may reflect an effort to evade US sanctions laws; The agreement requires HSBC to implement more robust risk-based AML and BSA procedures for conducting due diligence of potential new business entities in connection with mergers and acquisitions, including by involving audit, compliance, and legal personnel in the due diligence process.

In addition to forfeiting US\$1.256bio as part of its DPA, HSBC also agreed to pay US\$665mio in civil penalties – US\$500mio to the OCC and US\$165mio to the Federal Reserve – for its AML programme violations. The OCC penalty also satisfies a US\$500mio civil penalty to FinCEN. The bank's US\$375mio settlement agreement with OFAC is

satisfied by the forfeiture to DoJ.

As required by the DPA, HSBC also has committed to undertake enhanced AML and other compliance obligations and structural changes within its entire global operations to prevent a repeat of the conduct that led to this prosecution. HSBC has replaced almost all of its senior management, "clawed back" deferred compensation bonuses given to its most senior AML and compliance officers, and has agreed to partially defer bonus compensation for its most senior executives – its group general managers and group managing directors – during the period of the five-year DPA. In addition to these measures, HSBC has made significant changes in its management structure and AML compliance functions that increase the accountability of its most senior executives for AML compliance failures.

According to court documents, from 2006 to 2010, HSBC Bank USA severely understaffed its AML compliance function and failed to implement an anti-money laundering programme capable of adequately monitoring suspicious transactions and activities from HSBC Group Affiliates, particularly HSBC Mexico, one of HSBC Bank USA's largest Mexican customers. This included a failure to monitor billions of dollars in purchases of physical US dollars, or "banknotes," from these affiliates. Despite evidence of serious money laundering risks associated with doing business in Mexico, from at least 2006 to 2009, HSBC Bank USA rated Mexico as "standard" risk, its lowest AML risk category. As a result, HSBC Bank USA failed to monitor over US\$670bio in wire transfers and over US\$9.4bio in purchases of physical US dollars from HSBC Mexico during this period, when HSBC Mexico's own lax AML controls caused it to be the preferred financial institution for drug cartels and money launderers.

A significant portion of the laundered drug trafficking proceeds were involved in the Black Market Peso Exchange (BMPE), a complex money laundering system that is designed to move the proceeds from the sale of illegal drugs in the US to drug cartels outside of the US, often in Colombia. According to court documents, beginning in 2008, an investigation conducted by ICE Homeland Security Investigation's (HSI's) El Dorado Task Force, in conjunction with the US Attorney's Office for the Eastern District of New York, identified multiple HSBC Mexico accounts associated with BMPE activity and revealed that drug traffickers were depositing hundreds of thousands of dollars in bulk US currency each day into HSBC Mexico accounts. Since 2009, the investigation has resulted in the arrest, extradition, and conviction of numerous individuals

illegally using HSBC Mexico accounts in furtherance of BMPE activity.

As a result of HSBC Bank USA's AML failures, at least US\$881mio in drug trafficking proceeds – including proceeds of drug trafficking by the Sinaloa Cartel in Mexico and the Norte del Valle Cartel in Colombia – were laundered through HSBC Bank USA. HSBC Group admitted it did not inform HSBC Bank USA of significant AML deficiencies at HSBC Mexico, despite knowing of these problems and their effect on the potential flow of illicit funds through HSBC Bank USA.

According to court documents, from the mid-1990s through September 2006, HSBC Group allowed approximately US\$660mio in OFAC-prohibited transactions to be processed through US financial institutions, including HSBC Bank USA. HSBC Group followed instructions from sanctioned entities such as Iran, Cuba, Sudan, Libya and Burma, to omit their names from US dollar payment messages sent to HSBC Bank USA and other financial institutions located in the US. The bank also removed information identifying the countries from US dollar payment messages; deliberately used less-transparent payment messages, known as cover payments; and worked with at least one sanctioned entity to format payment messages, which prevented the bank's filters from blocking prohibited payments.

Specifically, beginning in the 1990s, HSBC Group affiliates worked with sanctioned entities to insert cautionary notes in payment messages including “care sanctioned country,” “do not mention our name in NY,” or “do not mention Iran.” HSBC Group became aware of this improper practice in 2000. In 2003, HSBC Group's head of compliance acknowledged that amending payment messages “could provide the basis for an action against [HSBC] Group for breach of sanctions.” Notwithstanding instructions from HSBC Group Compliance to terminate this practice, HSBC Group affiliates were permitted to engage in the practice for an additional three years through the granting of dispensations to HSBC Group policy.

Court documents show that as early as July 2001, HSBC Bank USA's chief compliance officer confronted HSBC Group's Head of Compliance on the issue of amending payments and was assured that “Group Compliance would not support blatant attempts to avoid sanctions, or actions which would place [HSBC Bank USA] in a potentially compromising position.” As early as July 2001, HSBC Bank USA told HSBC Group's head of compliance that it was concerned that the use of cover payments prevented HSBC Bank USA from confirming whether the underlying transactions

met OFAC requirements. From 2001 through 2006, HSBC Bank USA repeatedly told senior compliance officers at HSBC Group that it would not be able to properly screen sanctioned entity payments if payments were being sent using the cover method. These protests were ignored.

The US Senate's Permanent Subcommittee on Investigations held hearings in 2012 and released a 335-page report describing the bank's use of the US financial system to support Mexican drug cartels, terrorism supporters and Iran.

The report stated that HSBC marketed its New York payment operations to its global client base as a means for US dollar clearing, according to the report. HSBC affiliates operated in countries that included Mexico, Iran, the Cayman Islands, Saudi Arabia and Syria. Most of the USD payment transactions HSBC's US affiliate processed were for other HSBC affiliates, which were using the US affiliate almost exclusively for US dollar clearing.

For years, HSBC allowed non-US affiliates to omit or conceal information in US-bound transaction messages to evade the sanctions filter. To conceal the transactions, HSBC affiliates used a method called “stripping”, where references to Iran were deleted from records. HSBC affiliates also characterized the transactions as transfers between banks without disclosing the connection to Iran in what the Senate report called a “cover payment”. Between 2001 and 2007, more than 28,000 transactions were identified by an outside auditor for HSBC that potentially could have run afoul of laws that prohibit transactions with sanctioned countries. Of those, 25,000 involved Iran.

HSBC also provided global banking services, including US dollar clearing, to a Saudi-based Bank for decades despite evidence of the bank's relationship with global terrorist groups - the report said.

According to the report, the Saudi Bank was part of a network of Saudi-based banks and charities that funneled money to Al-Qaeda. In 2002, US agents searched the offices of a Saudi non-profit designated by the US as a terrorist organisation, Benevolence International Foundation. In that raid, agents uncovered a CD-ROM listing the names of financiers in Osama bin Laden's elite 'Golden Chain.' One of those names was a founder of a Saudi bank. The Golden Chain document is referenced by the 9-11 Commission's 2004 Report, media reports, US court filings and US Congressional hearings, though the Bank is not on any formal list and the Bank has denied all such allegations.

HSBC provided a wide range of banking services to the Saudi Bank, including wire transfers, trade finance, foreign exchange and asset management services. HSBC supplied large amounts of US\$ to the Saudi Bank through its US affiliate's Banknotes Department.

In 2005, HSBC's internal compliance officers asked that HSBC exit its relationship with the Saudi Bank. In 2005, US authorities sanctioned several Saudi organisations for terrorism support. These organisations were clients of the Saudi Bank but not the Saudi Bank. US investigations of one of the sanctioned organisations revealed that the organisation's senior officials cashed US\$130,000 in US travellers cheques at the Saudi Bank and used the money to support violent extremists in Chechnya. Some, but not all, HSBC employees acted to close accounts.

Four months later, HSBC officials reversed course, allowing affiliates to decide whether to continue to do business with the Saudi Bank. In late 2006, the Saudi Bank threatened to pull all of its business with HSBC unless it regained access to HSBC's bulk-cash transaction services. By the end of 2006, the relationship was completely reinstated, and HSBC continued to provide the bank with US dollars. HSBC agreed to continue to provide the bank bulk shipments of US dollars until 2010, when HSBC fully exited the bulk-cash business. In addition, at the Saudi Bank's request, HSBC expanded the relationship in January 2009, by authorising a Hong Kong office to supply the Saudi Bank with non-US currencies.

Additionally, the report described HSBC's provision of correspondent banking services to two other banks despite having information that both had alleged connections to terrorist groups through ownership.

UBS
2012 - US\$47.6mio¹⁵⁵
Agencies: UK FSA/FINMA

In November 2012, the UK FSA fined UBS £29.7mio (US\$47.6mio) for system and control failings that allowed Kweku Adoboli to cause over US\$2bio losses through unauthorized trading in London. The FSA Notice stated that, “UBS failed to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems, and failed to conduct its business from the London Branch with due skill, care and diligence.” For more details of this case see Kweku Adoboli in Part 2 Section 7, Criminal Cases above

At the same time in November 2012, FINMA published its findings, concluding that serious failings existed

in UBS' risk management and control environment. FINMA's conclusions were largely based on the internal report commissioned by UBS following the revelation of Adoboli's off-book trades. Its findings and conclusions largely mirrored those of the FSA, although it did go further than the FSA in some respects. Specifically, FINMA in addition criticized the Bank for a failure to formalise and communicate the ETF desk's reporting lines. It also explicitly censured the bank's reward and recognition systems, noting that despite several breaches of the bank's compliance policies relating to personal account dealing and spread betting, and repeated failures to comply with the bank's control standards, Adoboli was nonetheless highly remunerated, thereby incentivising his risk-seeking behaviour.

This went further than the FSA who made no specific findings on the culture at UBS (although they did make some oblique references, including to a suggestion that as those working in the middle office aspired to front office roles, they were more inclined to facilitate rather than challenge traders).

FINMA prohibited UBS from engaging in any new business activities without prior authorisation from the Swiss regulator.

Wegelin & Co
2012 - US\$58mio (forfeit) - shut down¹⁵⁶
Agency: DoJ

Wegelin & Co. was indicted in January 2012 on criminal charges alleging that the bank assisted wealthy Americans with concealing more than \$1.2 bio in secret accounts overseas. The charges against Wegelin were a superseding indictment of three Wegelin bankers on 3 January 2012 who were charged with fraud and conspiracy; and the indictment was the first time US authorities charged a bank rather than individuals with helping Americans evade taxes. It was reported that the US government seized over US\$16mio from Wegelin's correspondent banking account. The indictment alleges that Wegelin's bankers prospected the US clients that UBS had exited when they stopped servicing undeclared Swiss accounts. On 3 January 2013, Wegelin pleaded guilty and admitted it had helped wealthy Americans to evade at least US\$20mio in taxes. At its sentencing on 4 March, 2013, the court ordered a US\$22.05mio fine and ordered US\$20mio in further restitution, on top of US\$16.3mio already recovered in April 2012 by seizing money in its US correspondent account. Wegelin told clients that since they did not have a presence in the US they were not as likely to face US law enforcement pressure. Also, as Switzerland's oldest bank, they had a long tradition of secrecy and their

undeclared accounts would not be disclosed to the US authorities. The charges offer insight on how Wegelin allegedly attempted to solicit business from the US clients leaving UBS, and how they could charge high fees due to the clients' fear of criminal prosecution. The indictment outlines how: Wegelin used a special code, "BNQ," on around 70 new US undeclared accounts that were opened in 2008 and 2009. It also sometimes opened accounts for US citizens who held passports from other countries, and opened the accounts relying on non-US passports. Wegelin recruited US clients through a website, www.SwissPrivateBank.com, that was run by an unidentified third party. The website boasted there that "Swiss bank secrecy is not lifted for tax evasion. Neither the Swiss government nor any other government can obtain information about your bank account." Wegelin gave accounts special names, including "Elvis" and "Limpopo Foundation." The charges detailed the bank's work for nearly three dozen American clients, known only as clients A through JJ and also used sham companies and foundations formed under the laws of Liechtenstein, Panama and Hong Kong to provide secrecy. Wegelin encouraged clients not to come forward to the US Internal Revenue Service and disclose their names in exchange for reduced penalties. Wegelin assisted two unnamed Swiss banks to repatriate undeclared funds to their own US taxpayer clients by issuing cheques drawn on, and executing wire transfers through, its US correspondent bank account. In doing so, the bank sometimes separated the transactions into batches of cheques or multiple wire transfers in amounts that were less than US\$10,000 and comingled with unrelated funds to reduce the risk that the IRS would detect the undeclared accounts.

Special Focus 23 ING Bank

2012 - US\$619mio CMP^{157/158}
Agencies: DoJ, OFAC

In June 2012, Dutch bank ING agreed to a US\$619mio settlement for violations of US sanctions laws - the largest settlement for US sanctions violations at that time. The settlement resolved a two-year investigation into ING's intentional manipulation and deletion of information about Cuba, Iran and other US sanctions targets in transactions routed through US banks between 2002 and 2007. This "stripping activity" involved more than 20,000 financial and trade transactions totaling more than US\$1.6 bio.

US court documents describe how ING profited by

courting business from sanctioned entities like Iran and Cuba. Its clients in Cuba included a range of people, from individuals who wanted to cash US travellers' cheques to government ministries. It also engaged in transactions with Iran's central bank and state-owned National Iranian Oil Co.

ING's Wholesale Banking Division created policies for removing references in US-bound payments to Cuba and other countries sanctioned by the US. It created payment processing manuals to instruct employees on this practice and reprimanded employees for failing to follow these procedures. Beginning in the 1990s, senior bank management instructed employees in Curacao to omit references to Cuba in payment messages sent to the US to prevent US banks from stopping the transactions. Payments stopping in ING's filter because of references to Cuba were then stripped of information. For documentary trade transactions, ING arranged with paying banks and clients for the use of codes in settlement instructions to hide the involvement of a Cuban party. Additionally, ING's Curacao office increasingly used a type of bank-to-bank payment message format, an MT202, to send Cuba-related payments to US banks. The MT202 SWIFT message format in use during this time was not structured to provide the underlying transaction's beneficiary and remitter information.

While ING's US offices were not involved, several of its other branches also engaged in removing, omitting or hiding information in US bound payments. In 2003, ING's Trade and Commodity Finance's Romanian branch colluded with Iran's Bank Tejarat to remove details from trade finance documentation involving a US supplier to finance the exportation of US-origin goods to Iran. ING Bank's senior management in France oversaw the use of fraudulent endorsement stamps for use by Cuban financial institutions in processing travellers' cheque transactions, which disguised the involvement of Cuban banks in these transactions when they were processed through the US. ING Bank's Trade and Commodity Finance business at its Wholesale Banking branch in the Netherlands routed payments made on behalf of US-sanctioned Cuban clients through other corporate clients to obscure the sanctioned clients' identities.

Special Focus 24 Standard Chartered

2012 - US\$667mio¹⁵⁹⁻¹⁶³
Agencies: NY DFS, OFAC, Fed, DoJ, DANY

A New York bank regulator surprised the banking industry by threatening to pull British-based Standard Chartered's New York banking license because of the bank's concealment of more than 60,000 transactions involving Iran from US banks. In August 2012, New York's Department of Financial Services (DFS) ordered Standard Chartered to appear at a hearing to explain why it should keep its banking license. News of the order was reported on the front page of the Financial Times, the Wall Street Journal and other media sources. On the day the order was announced, Standard Chartered's share price plummeted.

The order described Standard Chartered's development and maintenance of automated processes to strip references to Iran from US bound payment messages. This practice allowed Iranian clients a way to evade US banks' OFAC sanctions filters and thus gain access to the US financial system. Internal emails revealed that senior management were aware of the stripping activity and refused to terminate it. The order quoted a senior Standard Chartered executive's reply to internal challenges to these practices, a reply that became instantly famous: "You f*cking Americans. Who are you to tell us, the rest of the world, that we're not going to deal with Iranians".

Eight days after the order was announced, and a day before the license hearing, Standard Chartered agreed to pay the New York regulator US\$340mio to settle the allegations that it concealed from US banks its use of those banks to process US\$250bio of transactions for Iranian clients. The loss of its New York banking license would have effectively barred the bank's direct access to the US financial system.

The settlement followed Standard Chartered's strong denial of having schemed with the Iranian government to launder US\$250bio through the US financial system. The bank pointed out that that non-US banks' initiation of "U-turn" transactions through New York to dollarize Iran-related transactions were permissible up until 2008. However, the NY regulator's preliminary findings of violations were based on New York State "books and records" requirements, not the federal OFAC sanctions regulations.

The New York regulator acted alone, but prominent members of the US Congress applauded the state regulator's ability to act quickly. Standard Chartered was already the subject of a separate probe dating to 2010 involving the US Treasury, the Federal Reserve Bank, the Justice Department and the Manhattan District Attorney to determine if Standard Chartered violated the OFAC regulations.

Days after the order was announced, victims of the 1983 Iran-sponsored terrorist bombing of US Marine barracks in Lebanon filed a civil suit against Standard Chartered in the US District of New York. In the suit, the plaintiffs allege that Standard Chartered conspired with Iran to hide assets and evade their 2007 US\$2.7bio default judgment.

In December 2012, Standard Chartered settled with DoJ, the New York District Attorney's Office (DANY), OFAC and the Fed in connection with apparent violations of multiple sanctions programmes for an aggregate penalty of US\$327mio. The US\$327mio included US\$227mio to DoJ/DANY; OFAC's fine of US\$132mio, which was deemed satisfied by the payment of the fines assessed by the US federal/county officials; and a US\$100mio fine imposed separately by the Fed. The December settlement by Standard Chartered is in addition to Standard Chartered's settlement and payment of a US\$340mio fine to the NY DFS in August of 2012. Standard Chartered's combined fine of US\$667mio is now the highest total fine in the continuing series of OFAC-related cases against non-US banks.

First Bank of Delaware
2012 - US\$15mio¹⁶⁴
Agencies: FDIC, FinCen

FDIC and FinCEN determined that the bank failed to implement an effective BSA/AML Compliance Programme with internal controls reasonably designed to detect and report evidence of money laundering and other suspicious activity. Specifically, the bank failed to adequately oversee third-party payment processor relationships and related products and services in a manner commensurate with associated risks. The civil money penalty is the result of the bank's history of non-compliance with laws and regulations and its numerous violations of the BSA.

Allianz
2012: US\$12.3mio¹⁶⁵
Agency: US SEC

Allianz, Germany-based insurance and asset management

company agreed to pay more than US\$12.3mio to settle SEC's corruption charges. "Allianz's subsidiary created an 'off-the-books' account that served as a slush fund for bribe payments to foreign officials to win insurance contracts worth several million dollars," said Kara Brockmeyer, Chief of the SEC Enforcement Division's FCPA Unit. The SEC's investigation uncovered 295 insurance contracts on large government projects that were obtained or retained by improper payments of US\$650,626 by Allianz's subsidiary in Indonesia to employees of state-owned entities. Allianz made more than US\$5.3mio in profits as a result of the improper payments. According to the SEC's order instituting settled administrative proceedings against Allianz, the misconduct occurred from 2001 to 2008 while the company's shares and bonds were registered with the SEC and traded on the New York Stock Exchange. Two complaints brought the misconduct to Allianz's attention. The first complaint submitted in 2005 reported unsupported payments to agents, and a subsequent audit of accounting records at Allianz's subsidiary in Indonesia uncovered that managers were using "special purpose accounts" to make illegal payments to government officials in order to secure business in Indonesia. The misconduct continued in spite of that audit. According to the SEC's order, the second complaint was made to Allianz's external auditor in 2009. Allianz failed to properly account for certain payments in their books and records. The improper payments were disguised in invoices as an "overriding commission" for an agent that was not associated with the government insurance contract. In other instances, the improper payments were structured as an overpayment by the government insurance contract holder, who was later "reimbursed" for the overpayment. Excess funds were then paid to foreign officials who were responsible for procuring the government insurance contracts. Allianz lacked sufficient internal controls to detect and prevent the wrongfull payments and improper accounting.

Special Focus 25 Libor Bid Rigging Scandal

**2012-2013: Fines so far: US\$6bio, US\$3.7bio by Regulators/US\$2.33bio by Competition Authorities,^{166/167}
Agencies: US DOJ, US CFTC, UK FSA, EU Commission**

The London Interbank offered Rate ("Libor") bid rigging scandal has so far exposed activities by a number of Libor benchmark setting banks to manipulate the London interbank offered rate, or Libor, as well as other benchmark rates, which together serve as the basis for interest rates on hundreds of trillions of dollars of financial instruments, with the prospect of more to come. In 2012, Barclays

(US\$455mio) and UBS (US\$1.5bio) and in 2013 Royal Bank of Scotland (US\$612mio), ICAP (US\$87mio) and Rabobank (US\$1.05bio) all admitted traders had acted improperly. EU Competition Authorities have also levied fines (see later).

The manipulation goes back mainly to 2007 to the start of the financial crises with suspicions first raised in 2008 by The Wall Street Journal (WSJ) suggesting that some banks, concerned about the negative implications of reporting borrowing costs, had instead understated borrowing costs which fed into Libor setting during the period. Whilst both the British Bankers Association (BBA), and the Bank for International Settlements at the time rejected these suggestions. The then Governor of the Bank of England, Mervyn King, by the end of 2008, described Libor to the UK Parliament saying "It is in many ways the rate at which banks do not lend to each other, .. it is not a rate at which anyone is actually borrowing," and released minutes from the Bank of England showed that as early as November 2007, the BoE deputy governor Paul Tucker was aware of industry concerns that the Libor rate was being underreported.

Across the Atlantic, documents since released in 2012, dating back to 2007 showed that The New York Federal Reserve were aware that some banks were understating their borrowing costs when setting Libor and chose to take no action against them at that time. In a released 2008 document a Barclays employee told the New York Fed, "We know that we're not posting an honest Libor, and yet we are doing it, because if we didn't do it, it draws unwanted attention on ourselves." Released documents also show that in early 2008 a memo written by then New York Fed President Tim Geithner to Bank of England chief Mervyn King looked into ways to "fix" Libor.

It is now clear that the turmoil in the markets following the financial crises had serious consequences for the validity of Libor.

A detailed study by economists, Snider and Youle, in April 2010, however, publicly corroborated the results of the earlier Wall Street Journal study that the Libor submissions by some member banks were being understated. Unlike the earlier study, Snider and Youle suggested that the reason for understatement by member banks was not simply that some of the banks were trying to appear strong, especially during the financial crisis starting in 2007, but rather that the banks sought to make substantial profits on their large Libor interest-linked portfolios. This put the nature of possible actions into a new light and led to comprehensive investigations to learn the truth.

Barclays Bank¹⁶⁸

In 2012, Barclays agreed to pay US\$455 mio for its role in

the scandal, with investigations revealing that traders had rigged the Libor rate which is the benchmark for more than \$360 trillion of securities. The CFTC imposed a penalty of US\$200 million, in addition, as part of an agreement with the DOJ, Barclays admitted to its misconduct and agreed to pay a penalty of US\$160 million with the FSA levying a fine of US\$95mio(£59.5 million). Following public outrage, Marcus Agius, Chairman of Barclays, resigned from his position, and one day later, Bob Diamond, the Chief Executive officer of Barclays. Bob Diamond was subsequently questioned by the Parliament of the UK regarding the manipulation of Libor rates. He said he was unaware of the manipulation until that month, but mentioned discussions he had with Paul Tucker, deputy governor of the Bank of England. Tucker then voluntarily appeared before parliament, to clarify the discussions he had with Bob Diamond. He said he had never encouraged manipulation of Libor, and that other self-regulated mechanisms like the Libor should be reformed.

According to the FSA, Barclays' misconduct included: making submissions which formed part of the Libor and EURIBOR setting process that took into account requests from Barclays' interest rate derivatives traders. These traders were motivated by profit and sought to benefit Barclays' trading positions; seeking to influence the European Interbank Offered Rate ("EURIBOR") submissions of other banks contributing to the rate setting process; and reducing its Libor submissions during the financial crisis as a result of senior management's concerns over negative media comment. In addition, Barclays failed to have adequate systems and controls in place relating to its Libor and EURIBOR submissions processes until June 2010 and failed to review its systems and controls at a number of appropriate points. Barclays also failed to deal with issues relating to its Libor submissions when these were escalated to Barclays' Investment Banking compliance function in 2007 and 2008. Tracey McDermott, acting director of enforcement and financial crime, said:

"Barclays' misconduct was serious, widespread and extended over a number of years. The integrity of benchmark reference rates such as Libor and EURIBOR is of fundamental importance to both UK and international financial markets. Firms making submissions must not use those submissions as tools to promote their own interests." "Making submissions to try to benefit trading positions is wholly unacceptable. This was possible because Barclays failed to ensure it had proper controls in place. Barclays' behaviour threatened the integrity of the rates with the risk of serious harm to other market participants." "The FSA continues to pursue a number of other significant cross-border investigations in this area and the action we have taken against Barclays should leave firms in no doubt about the serious consequences of this type of failure."

UBS¹⁶⁹

On 19 December 2012, UBS agreed to pay regulators US\$1.5bio (US\$1.2bio to the US Department of Justice and the Commodity Futures Trading Commission, £160mio to the UK Financial Services Authority and 60m CHF to the Swiss Financial Market Supervisory Authority) for its role in the scandal. The investigation revealed that UBS traders had colluded with other panel banks and had made over 2,000 written requests for movements in rates from at least January 2005 to at least June 2010 to benefit their trading positions. According to transcripts released by the UK's Financial Services Authority, UBS traders also offered financial inducements to interdealer brokers to help manipulate rates by spreading false information. US Assistant Attorney General Lanny Breuer described the conduct of UBS as "simply astonishing" and declared the US would seek, as a criminal matter, the extradition of traders Tom Hayes and Roger Darin. UBS's settlement also included an agreement for its Japanese unit to plead guilty to wire fraud.

Royal Bank of Scotland¹⁷⁰

In 2013, the third Bank involved in the Libor bid rigging scandal was announced with a global settlement when, Royal Bank of Scotland (RBS) agreed to pay a combined US\$612mio, including US\$325mio to the US Commodities Futures Trading Commission, US\$150mio to the DOJ and US\$137 to the UK Financial Services Authority. RBS Securities Japan Limited also pleaded guilty to one count of US wire fraud and admitted its role in manipulating the Japanese Yen Libor and participating in a price-fixing conspiracy.

ICAP¹⁷¹

In September 2013 the fourth Financial Institution involved in the Libor bid rigging scandal was revealed. US and UK authorities fined brokerage firm ICAP US\$87mio for its role in manipulating benchmark interest rates, in particular, Libor. As part of the agreement, ICAP will pay the U.S. Commodity Futures Trading Commission US\$65mio and the U.K.'s Financial Conduct Authority £14mio (US\$22mio).

In addition, the US Department of Justice (DOJ) also announced that it was charging three former ICAP brokers, claiming they engaged in criminal fraud related to the Libor scandal. The DOJ charged Darrell Reed, Daniel Wilkinson and Colin Goodman with conspiracy to commit wire fraud and two counts of wire fraud. They each face a maximum penalty of 30 years in prison. "By allegedly participating in a scheme to manipulate benchmark interest rates for financial gain, these defendants undermined the integrity of the global markets," Attorney General Eric Holder said in a statement. "They were supposed to be honest brokers, but instead, they put their own financial interests ahead of that larger responsibility. And as a result, transactions and finan-

cial products around the world were compromised, because they were tied to a rate that was distorted due to the brokers' dishonesty. These charges underscore the Justice Department's determination to hold accountable all those whose conduct threatens the integrity of our financial markets."

London-based ICAP is the world's largest interdealer broker, which acts as a middleman between major financial institutions. In the Libor case, some brokers, including those at ICAP, allegedly took instructions from bank traders about which direction they wanted Libor to move, and they passed those requests on to other banks. Authorities say that allowed Libor rigging to become a widespread phenomenon rather than a series of isolated efforts by individual bank traders

Authorities disclosed electronic communications among those charged. The released excerpts show the brokers allegedly writing about "managing to fudge" Libor, of receiving "kick backs" and bottles of champagne. One broker referred to himself as "Lord Libor" and "Mr. Libor" according to the UK and US settlements. The rewards given to the brokers for their allegedly corrupt conduct ranged from "copious amounts of curry" to tens of thousands of dollars in cash, according to settlement documents. "The motivation for this scheme was nothing short of pure greed," said David Meister, Director of Enforcement at the CFTC.

In a July 2007 electronic chat, one of the ICAP brokers told a colleague that he had "promised to line pockets with silver" if Mr..... could move one type of Libor higher on behalf of a lucrative trading client, according to an excerpt published by the Justice Department.

The ICAP brokers were especially interested in pleasing a derivatives trader who at the time worked in Tokyo for UBS, the settlements state. That trader, Tom Hayes, has been criminally charged in the US and UK. Mr. Hayes was a coveted client for ICAP and other brokerages because he brought them a lot of business. At times, though, the brokers grumbled that they were being insufficiently compensated for the work they were doing.

"With UBS how much does [Mr. Hayes] appreciate the yen Libor scoop?" one broker allegedly wrote in an April 2007 email to another disclosed by the Justice Department. He added: "It seems to me that he has all the glory etc....I get the dribs and drabs. Life is tough enough over here without having to double guess the Libors every morning and get zipper-de-do-da."

Rabobank^{172/173}

US and European regulators fined Dutch lender Rabobank US\$1.05bio for rigging benchmark interest rates, making it the fifth bank punished so far, after 30 staff were involved

in "inappropriate conduct". The bank's Chief Executive Piet Moerland resigned, saying he was shocked by language revealed in emails exchanged by staff involved over six years to 2011. Japan's banking regulator also criticized the Tokyo branch of Rabobank, with Rabobank reacting with closing its branch in Japan. Rabobank failed to act after an employee responsible for submitting the bank's yen-denominated Libor rates told an internal audit group in 2009 his submissions were based on instructions from traders. One of the regulators, the UK FCA found over 500 instances of attempted Libor manipulation, directly or indirectly, involving at least nine managers and 19 other individuals based across the world.

European Commission Action

The European Commission fined 8 international financial institutions a total of €1.7bio for participating in illegal cartels in Euro interest rate derivatives (EIRD), and in Yen interest rate derivatives (YIRD).

The EIRD cartel operated between September 2005 and May 2008. The settling parties were Barclays, Deutsche Bank, RBS and Société Générale. The cartel aimed at distorting the normal course of pricing components for these derivatives. Traders of different banks discussed their bank's submissions for the calculation of the EURIBOR as well as their trading and pricing strategies. The Commission's investigation started with unannounced inspections in October 2011. The Commission opened proceedings in March 2013. Barclays was not fined as it benefited from immunity under the Commission's 2006 Leniency Notice for revealing the existence of the cartel to the Commission. Deutsche Bank, RBS and Société Générale received a reduction of their fines for their cooperation in the investigation under the Commission's leniency programme. These companies received a further fine reduction of 10% for agreeing to settle the case with the Commission. In the context of the same investigation, proceedings were opened against Crédit Agricole, HSBC and JP Morgan and the investigation continues.

In the Yen interest rate derivatives (YIRD) sector, the Commission uncovered 7 distinct bilateral infringements lasting between 1 and 10 months in the period from 2007 to 2010. The collusion included discussions between traders of the participating banks on certain JPY LIBOR submissions. The traders involved also exchanged, on occasions, commercially sensitive information relating either to trading positions or to future JPY LIBOR submissions (and in one of the infringements relating to certain future submissions for the Euroyen TIBOR – Tokyo interbank offered rate). The banks involved in one or more of the infringements were UBS, RBS, Deutsche Bank, Citigroup and JP

Morgan. The broker RP Martin facilitated one of the infringements by using its contacts with a number of JPY LIBOR panel banks that did not participate in the infringement, with the aim of influencing their JPY LIBOR submissions.

The Commission opened proceedings in February 2013. UBS received full immunity under the Commission's 2006 Leniency Notice for revealing to the Commission the existence of the infringements. Citigroup also benefited from full immunity for its participation in one bilateral infringement. For their cooperation with the investigation, the Commission granted fine reductions to Citigroup, Deutsche Bank, RBS and RP Martin, under the Commission's leniency programme. The Commission has also opened proceedings against the cash broker ICAP, which continues.

In setting the level of fines, the Commission took into account the banks' value of sales within the EEA, the serious nature of the infringements, their geographic scope and respective durations.

As far as the EIRD cartel, the fines imposed are as follows: Barclays - None (due to whistle blowing- avoiding €690mio fine); Deutsche Bank - €465.8mio; Société Générale - €445.8mio; and RBS - €131mio;

As far as the YIRD cartels, the fines imposed are as follows: UBS - None (due to whistle blowing- avoiding €2.5bio); RBS - €260mio; Deutsche Bank - €259.5 mio; JP Morgan - €79.9 mio; Citigroup - €70mio (avoided €55mio in addition); and RP Martin - €247,000.

National Bank Abu Dhabi

2012: US\$855,000¹⁷⁴

Agency: US OFAC

National Bank of Abu Dhabi ("NBAD") paid US\$855,000 to settle with OFAC for violations of OFAC regulations relating to Sudan. NBAD provided information to OFAC revealing that certain of its clerical staff removed or omitted Sudan-related references in 45 payment instructions processed on behalf of its Sudan branch for payments routed through financial institutions located in the US. The transactions occurred between 2004 to 2005.

MoneyGram

2012: US\$100mio DPA¹⁷⁵

Agency: US DoJ

Moneygram International Inc. a global money services business headquartered in Dallas entered into a Deferred Prosecution Agreement with the US DoJ and forfeited

US\$100mio for Anti-Money Laundering and Wire Fraud Violations. MoneyGram admitted to criminally aiding and abetting wire fraud and failing to maintain an effective anti-money laundering programme. According to court documents, MoneyGram was involved in mass marketing and consumer fraud phishing schemes, perpetrated by corrupt MoneyGram agents and others, that defrauded tens of thousands of victims in the US. MoneyGram also failed to maintain an effective anti-money laundering programme in violation of the Bank Secrecy Act.

"MoneyGram's broken corporate culture led the company to privilege profits over everything else," said Assistant Attorney General Breuer. "MoneyGram knowingly turned a blind eye to scam artists and money launderers who used the company to perpetrate fraudulent schemes targeting the elderly and other vulnerable victims. In addition to forfeiting US\$100mio, which will be used to compensate victims, MoneyGram must for the next five years retain a corporate monitor who will report regularly to the Justice Department."

As part of the DPA, MoneyGram has agreed to enhanced compliance obligations and structural changes to prevent a repeat of the charged conduct, including: the creation of an independent compliance and ethics committee of the board of directors with direct oversight of the chief compliance officer and the compliance programme; the adoption of worldwide anti-fraud and anti-money laundering standards to ensure all MoneyGram agents throughout the world will, at a minimum, be required to adhere to US anti-fraud and anti-money laundering standards; the adoption of a bonus system which rates all executives on success in meeting compliance obligations, with failure making the executive ineligible for any bonus for that year; and the adoption of enhanced due diligence for agents deemed to be high risk or operating in a high-risk area.

To oversee implementation and maintenance of these enhanced compliance obligations and evaluate the overall effectiveness of its anti-fraud and anti-money laundering programmes, MoneyGram has agreed to retain an independent corporate monitor who will report regularly to the Justice Department. Under the DPA, the department will recommend the dismissal of the criminal information in five years, provided MoneyGram fully abides by the DPA's terms.

According to court documents, starting in 2004 and continuing until 2009, MoneyGram violated US law by processing thousands of transactions for MoneyGram agents known to be involved in an international scheme to defraud members of the US public. MoneyGram profited from the scheme by collecting fees and other revenues on the fraudulent transactions. The scams, which generally

targeted the elderly and other vulnerable groups, included posing as victims' relatives in urgent need of money and falsely promising victims large cash prizes, various high-ticket items for sale over the Internet at deeply discounted prices or employment opportunities as "secret shoppers." In each case, the perpetrators required the victims to send them funds through MoneyGram's money transfer system. Despite thousands of complaints by customers who were victims of fraud, MoneyGram failed to terminate agents that it knew were involved in scams. As early as 2003, MoneyGram's fraud department would identify specific MoneyGram agents believed to be involved in fraud schemes and recommended termination of those agents to senior management. These termination recommendations were rarely accepted because they were not approved by executives in the sales department and, as a result, fraudulent activity grew from 1,575 reported instances of fraud by customers in the US and Canada in 2004 to 19,614 reported instances in 2008. Cumulatively, from 2004 through 2009, MoneyGram customers reported instances of fraud totaling at least US\$100mio.

The USPIS and US Attorney's Office for the Middle District of Pennsylvania have been investigating and prosecuting telemarketing scams that used MoneyGram's money transfer system and corrupt MoneyGram agents since 2007. To date, the US Attorney's Office for the Middle District of Pennsylvania has brought conspiracy, fraud and money laundering charges against 28 former MoneyGram agents.

US Attorney Smith said, "Thousands of citizens in Pennsylvania and other states suffered heartbreaking financial losses for years because of these international telemarketing schemes which depended on MoneyGram's facilities to give them an electronic highway to move their illegal profits quickly out of the country. The determined work of US Postal Inspectors and federal prosecutors disrupted and closed that electronic highway, hopefully for good. This case provides a way to get restitution for victims and ensure that MoneyGram does its part to deter similar scams in the future."

MoneyGram's involvement in this international fraud scheme resulted from a systematic, pervasive, and wilful failure to meet its anti-money laundering (AML) obligations under the Bank Secrecy Act (BSA). Court documents show that MoneyGram failed to meet its AML obligations by, among other things, failing to: implement policies or procedures governing the termination of agents involved in fraud and/or money laundering; implement policies or procedures to file the required Suspicious Activity Reports (SARs) when victims reported fraud to MoneyGram on transactions over US\$2,000; file SARs on agents MoneyGram knew were involved in the fraud; conduct effective AML audits of its agents and outlets; conduct adequate due diligence on

prospective and existing MoneyGram Agents by verifying that a legitimate business existed; and Sufficiently resource and staff its AML programme.

MoneyGram's BSA failures spanned five years, and resulted, among other things, from the failure of its fraud and AML compliance functions to share information and from its regularly resolving disagreements between its sales and fraud departments in the sales department's favour. One notable such disagreement occurred in April 2007, when, at a meeting attended by senior MoneyGram executives, the fraud department recommended that 32 specific Canadian agents that were characterized as "the worst of the worst" in terms of fraud be immediately closed. The sales department disagreed with the fraud department's recommendation, and these outlets were not closed; instead, MoneyGram continued to process transactions from the 32 outlets despite continued complaints of fraud.

SAC Capital

2013 - US\$1.8bio (3 cases: 1 - US\$602mio/2 - US\$14mio/3 - US\$1.2bio)¹⁷⁶

Agency: SEC and others

A US hedge fund, SAC Capital Group agreed in March 2013 to pay US\$602mio and US\$14mio to settle SEC charges that it participated in insider trading schemes. The main case involved a clinical trial for an Alzheimer's drug being jointly developed by two pharmaceutical companies. The SEC had charged CR Intrinsic with insider trading in November 2012, alleging that one of the firm's portfolio managers Mathew Martoma illegally obtained confidential details about the clinical trial from Dr Sidney Gilman, who was selected by the pharmaceutical companies, Elan Corporation and Wyeth, who served as chairman of the safety monitoring committee overseeing the trial and who was to present the final drug trial results to the public. The settlement amount is the largest ever in an insider trading case, requiring CR Intrinsic, an affiliate of SAC Capital Advisors, to pay US\$274,972,541 in disgorgement, being the amount made on the inside information, US\$51,802,381.22 in prejudgment interest, and a US\$274,972,541 penalty. "The historic monetary sanctions against CR Intrinsic and its affiliates are sharp warning that the SEC will hold hedge fund advisory firms and their funds accountable when employees break the law to benefit the firm," said George S. Canellos, Acting Director of the SEC's Division of Enforcement. Sanjay Wadhwa, Senior Associate Director of the SEC's New York Regional Office, added, "A robust culture of compliance and zero tolerance toward employee misconduct can help other firms avoid the severe financial consequences that CR Intrinsic is facing for its misconduct."

The SEC's complaint against CR Intrinsic, Martoma, and

Dr. Gilman alleged that during phone calls arranged by a New York-based expert network firm for which Dr. Gilman moonlighted as a medical consultant, he tipped Martoma with safety data and eventually details about negative results in the trial about two weeks before they were made public in July 2008. Martoma and CR Intrinsic then caused several hedge funds to sell more than US\$960mio in Elan and Wyeth securities in a little more than a week.

Fast Forward to 2013 and SAC Capital faced more trouble, when it was charged criminally by the Manhattan US Attorney's office for insider trading. After a multiyear investigation conducted by the U.S. Attorney's Office, the FBI, and the Securities and Exchange Commission, a grand jury indicted SAC Capital, accusing the firm of fostering a culture where employees engaged in rampant securities fraud. The indictment said traders at SAC engaged in insider trading that was "substantial, pervasive, and on a scale without known precedent in the hedge fund industry." Manhattan US Attorney Preet Bharara described SAC as "a magnet for market cheaters." In addition to charges against the hedge fund, charges were laid against founder Steven Cohen, by the SEC for failure to supervise two employees who faced trial for insider trading. As a result SAC Capital agreed to a guilty plea for securities fraud and to pay a fine amounting in total to US\$1.8bio (which includes the US\$616mio already paid). As part of the settlement, SAC will lose the right to manage public money, by surrendering its investment-advisor registration with the SEC, and it will redeem the rest of the public money it currently manages. SAC will then convert to a family office that manages at least US\$9 billion. Despite the settlement, SAC will still have open separate civil charges, levied by the SEC, that company founder Steve Cohen failed to supervise employees who engaged in insider trading.

EFG Private Bank

2013 - £4.2 mio (US\$6.4mio)¹⁷⁷

Agency: UK FCA

The UK Financial Conduct Authority (FCA), formerly the FSA fined EFG Private Bank Ltd £4.2 million for failing to take reasonable care to establish and maintain effective anti-money laundering (AML) controls for high risk customers. The failings were serious and lasted for more than three years.

EFG is the UK private banking subsidiary of the EFGI Group, a global private banking group, based in Switzerland. EFG provides private banking and wealth management services to high net worth individuals including some from overseas jurisdictions recognised as presenting a higher risk of money laundering and/or bribery and corruption. At the end of 2011 around 400 of EFG's 3,342 customer accounts were deemed by the firm to present a higher risk

of money laundering or reputational risk, and of these 94 were held by politically exposed persons (PEPs).

During an FSA inspection in 2011, the FSA found that EFG had not fully put its AML policies into practice. Of particular concern was that 17 of 36 reviewed customer files, opened between December 2007 and January 2011, contained customer due diligence that highlighted significant money laundering risks, but insufficient records of how the bank's senior management had mitigated those risks. Of these 17 files, the FSA found that the risks highlighted in 13 files related to allegations of criminal activity or that the customer had been charged with criminal offences including corruption and money laundering. For example, in one account, EFG's due diligence highlighted that a prospective client had acquired their wealth through their father, about whom there were allegations of links with organised crime, money laundering and murder. However there was insufficient information on file to explain how the bank concluded that this risk was acceptable or how it was mitigating the risks. EFG also failed to appropriately monitor its higher risk accounts. Of the 99 PEP and other high risk customer files reviewed by the FSA, 83 raised serious concerns about EFG's monitoring of the relationship.

Tracey McDermott, head of enforcement and financial crime, said: "Banks are the first line of defence to make sure that proceeds of crime do not find their way into the UK. In this case while EFG's policies looked good on paper, in practice it manifestly failed to ensure that it was addressing its AML risks. Its poor implementation of its agreed policies risked the bank handling the proceeds of crime. These failures merited a strong penalty from the FCA. Firms that accept business from high risk customers must have systems, controls and practices to manage that risk. The FCA will continue to focus on high risk customers and business." EFG settled at an early stage of the investigation and qualified for a 30% discount on its fine. Without the discount the fine would have been £6mio.

UBS France

2013 - US\$13mio (€10mio)¹⁷⁸

Agency: French ACP

The French banking regulator, ACP, fined UBS France €10mio for according to it failing to tighten controls to curb money laundering and cross-border fiscal fraud. The ACP statement did not specify whether there had been any illicit activity, however. According to the ACP, UBS France was alerted to "grave suspicions" in 2007 of its sales force's possible involvement in illicit marketing and the covering up of tax fraud, waiting more than 18 months before setting up the necessary controls. The fine is more than twice the €4mio penalty the regulator demanded from Société Générale SA in 2008 because of internal-control shortcomings

related to Jerome Kerviel's multi-billion-euro trading loss. The UBS unit also failed to control its sales force's potential access to computer files shared with the parent company that could have been used to identify prospective clients for accounts outside France. In response UBS stated that "We disagree with many of the disciplinary commission's conclusions," adding that it will consider whether to appeal the decision. "UBS does not tolerate any activities intended to help its clients circumvent their tax obligations." UBS also stated that "This is an issue from the past and we are pleased to note that the disciplinary commission acknowledges in its report that UBS France SA has taken appropriate steps to strengthen its compliance framework since 2009."

HSBC Argentina

2013 - US\$1mio (& US\$20mio/2012)¹⁷⁹

Agency: Financial Crimes Unit/Argentina

Argentina's financial crimes unit fined the local unit of HSBC Holdings Plc (HSBA) US\$1mio for failing to report a suspicious transaction at the time, carried out in 2007. The case involved a client who moved five million pesos (about US\$941,530) into a bank account, with the money then withdrawn from the bank account over a month. Allegedly the client involved had no declared assets and a monthly income that was officially reported as less than US\$3,000. This is not the first time that HSBC has faced fines in Argentina. The financial crimes unit fined the bank US\$14mio and then another US\$6mio in 2012 for failing to report suspicious transactions.

HSBC Mexico SA

2013 - No Fine / License Revoked¹⁸⁰

Agency: The Cayman Islands Monetary Authority (CIMA)

The Cayman Islands Monetary Authority (CIMA) announced in March 2013 that it had revoked the licence of the HSBC Mexico SA Cayman Islands branch. The decision followed an investigation to determine whether the Cayman Islands branch had violated local money laundering laws and regulations. The investigation found that the bank was "conducting business in a manner detrimental to the public interest, the interest of its depositors or of the beneficiaries of any trust or other creditors and that the direction and management of its business has not been conducted in a fit and proper manner."

Bank of Tokyo Mitsubishi-UFJ Ltd (BTMU)

2013 - US\$258.5mio (US\$250mio & US\$8.5mio)^{181/182}

Agencies: The New York State Department of Financial Services (DFS) / OFAC

The Bank of Tokyo Mitsubishi-UFJ Ltd (BTMU) has agreed to pay US\$250 million to settle charges that it

breached New York state banking laws by moving an estimated US\$100bio through 28,000 USD clearing transactions through New York, for entities subject to international sanctions and entities on the US Department of the Treasury Office of Foreign Assets Control's list of specially designated nationals. According to the DFS, BTMU provided employees with written instructions on how to remove information from wire transfers that could have identified the entities and countries involved. DFS financial services superintendent Benjamin Lawsky said the DFS will "continue to take a hard line in rooting out misconduct at banks that threatens our national security" and "will take strong enforcement action to protect our country from money laundering, terrorism, and other dangerous misdeeds". BTMU said in a statement that it "voluntarily and promptly" stopped the practices when they came to light in 2007 and has subsequently "significantly" improved its compliance policies and procedures. BTMU had a year earlier in 2012 received a US\$8,571,634 fine from OFAC for the same matter. In 2007, BTMU's senior management learned of these practices, commenced an internal review of historical transaction data, and initiated a voluntary self-disclosure to the US authorities - OFAC. OFAC found that the apparent violations constituted an egregious case, because: BTMU's conduct concealed the involvement of U.S. sanctions targets and displayed reckless disregard for U.S. sanctions; the general manager of the Operations Centre in Tokyo knew or had reason to know that procedures had been implemented instructing employees to manipulate payment instructions; BTMU's conduct conferred a substantial economic benefit to targets of OFAC sanctions and BTMU is a large, commercially sophisticated financial institution. Nevertheless in its favour, BTMU had undertaken significant remediation to improve its OFAC compliance policies and procedures; BTMU substantially cooperated with OFAC's investigation, including providing detailed and organised information regarding the apparent violations, and entered into a tolling agreement with OFAC.

Barclays

2013 - US\$487.9mio¹⁸³

Agency: Federal Energy Regulatory Commission (FERC)

Barclays faced energy market manipulation charges, from the US Federal Energy Regulatory Commission who proposed a fine of US\$435mio and US\$34.9mio disgorgement from Barclays over the power trading market from late 2006 to 2008. The proposed fines were confirmed recently in 2013 as FERC found that Barclays traders flattened substantial monthly physical index positions of four of the then most liquid trading points in the western US for the fraudulent purposes of manipulating the index price to benefit Barclays' financial swap positions. FERC found that Barclays' actions demonstrated an alternative co-ordinated and intentional effort to carry out a manipulative scheme,

in violation of the Federal Power Act and FERC's Anti-Manipulation Rule.

Nordea AB

2013: US\$4.7mio fine¹⁸⁴

Agency: Sweden's Financial Supervisory Authority

The Nordic region's biggest bank, was fined by Sweden's Financial Supervisory Authority 30 million kronor (US\$4.7mio) for inadequate anti-money laundering and terrorism financing prevention procedures. Following investigations into the bank beginning in late 2009, the SFSA's conclusions ultimately came down to four regulatory areas: identifying and screening clients' beneficial owners; reporting transactions; "know your customer"; and internal governance and control.

The Fine cited Nordea's approach to a customer named Takilant Ltd. Takilant, a Gibraltar-based company, had been linked by Swedish prosecutors to a suspected bribery deal involving Swedish telecom operator TeliaSonera AB. The SFSA also criticised Nordea for failing to comply with EU regulations. SFSA Executive Director of the Banks Operational Section, Uldis Cerpšs stated that, "There were several risk indicators that we had outlined, which in combination should clearly signal heightened risk." "We share the FSA's view," Nordea press spokeswoman Helena Ostman said "We should have conducted a more thorough review [of Takilant]." Nordea has frozen Takilant's account, and has imposed stricter due diligence routines, she said. The bank, however, finds the penalty to be too large as no illegal transactions are believed to have taken place in the frozen accounts. The SFSA argues that for several years Nordea did not screen beneficial owners against the EU sanctions regulations, exposing itself to the risk of giving blacklisted individuals access to economic resources without its knowledge. The bank has also been deficient in its reporting to the SFSA regarding transactions in frozen accounts, the agency said. Takilant opened the account with Nordea Sweden in 2011, according to the bank.

Swedish prosecutors have been investigating allegations that telecom operator TeliaSonera AB engaged in money laundering connected to the acquisition in 2007 of an Uzbekistan wireless data license and other assets from Takilant. The prosecutors have claimed TeliaSonera knew that one of the partners in Takilant was the daughter of Uzbek president Islam Karimov. TeliaSonera in a statement in January denied it was aware of any beneficiaries from the deal other than Takilant's registered director. Uzbekistan is the world's eighth most corrupt country according to anti-corruption watchdog Transparency International, and the combination of a beneficial owner domiciled in that country and the hefty US\$20mio deposit in the account should have alerted Nordea to conduct enhanced due diligence such as a more

extensive background check of the owners, Mr Cerpšs said.

Panther Energy Trading

2013: US\$5.8mio¹⁸⁵

Agencies: US CFTC; CME; UK FCA

High Frequency trading makes up much of the volume on today's equity markets and has been identified as a particular risk for some time, albeit more to do historically with concerns about algorithmic trading leading to flash crashes and the like. High Frequency or Algorithmic Trading is essentially where traders use superfast computers to trade in milliseconds after news or markets start to move but ahead of the rest of the traditional market in order to capture the market news as quickly as possible. Still as with any other trading firm or trader manipulative techniques can be practiced and even hard-wired into algo trading and this is what US and UK regulators alleged against Panther Energy Trading and Michael Coscia, one of its chief traders. US and UK authorities have signalled their intent to focus on high-frequency trading and so this fine shouldn't be a surprise, still it is the first of its kind and clearly demonstrates that regulatory authorities are looking to crack down on market abuse in this area and to send a clear signal to the market as a result. The crackdown represents the first time the CFTC has used powers granted under the Dodd-Frank Act, and that the newly-created FCA has fined a high-frequency trading company.

The regulators allege Panther used practices such as spoofing and layering. These techniques are used to deliberately make and then cancel large amounts of orders to create a false impression of liquidity. For example, the CFTC said in the West Texas Intermediate crude oil market, Panther Energy placed a small, 17-contract sell order of US\$85.29 per barrel that underpriced other offers in the market. Within a fraction of a second, Panther then flooded the market with buy orders that it intended to cancel, driving the market towards its selling price. "The programme sought to capture an immediate profit from selling the 17 lots," the regulator said. The CFTC said Panther spoofed 18 separate US futures markets, including oil, soybeans and wheat, as well as interest rates and stock indices between August and October 2011. UK regulators said Panther also made thousands of false orders for crude oil and gas contracts on the ICE Futures Europe exchange.

"High-frequency trading and the use of algorithms are an important and commonplace part of the markets nowadays, but in this case these techniques were deliberately designed to abuse the market, undermining its integrity," said Tracey McDermott, the FCA's director of enforcement and financial crime. The CFTC ordered Michael Coscia, the trader at the centre of the allegations, to pay a total of US\$2.8mio in trading profits, while CME Group imposed

fines totalling US\$2.1mio. The CFTC also banned Panther and Mr Coscia from trading on any its registered entities for one year for offences in the US. The FCA imposed a fine of US\$903,000 (£597,000) and six-month trading ban on its exchanges.

Oppenheimer & Co., Inc

2013: US\$1.4mio CMP¹⁸⁶

Agency: Finra

FINRA fined Oppenheimer US\$1,425,000 for the sale of unregistered penny stock shares and for failing to have an adequate anti-money laundering (AML) compliance programme to detect and report suspicious penny stock transactions. Oppenheimer is also required to retain an independent consultant to conduct a comprehensive review of the adequacy of Oppenheimer's penny stock and AML policies, systems and procedures. Oppenheimer agreed to the sanctions to resolve charges first brought against the firm in a FINRA complaint in May 2013.

FINRA said, "Broker-dealers are required by federal securities laws and FINRA rules to monitor customers' accounts so that those accounts are not used for illegal activities, such as money laundering and penny stock schemes that can cause considerable harm to investors. If Oppenheimer had an adequate AML and supervisory programme in place, it would have made further inquiry into the penny stock sales that were the basis of this action." FINRA found that from 19 August 2008 to 20 September 2010, Oppenheimer, through branch offices located across the country, sold more than a billion shares of twenty low-priced, highly speculative securities (penny stocks) without registration or an applicable exemption.

The customers deposited large blocks of penny stocks shortly after opening the accounts, and then liquidated the stock and transferred proceeds out of the accounts. Each of the sales presented additional "red flags" that should have prompted further review to determine whether the securities were registered. FINRA also found that the firm's systems and procedures governing penny stock transactions were inadequate, and were unable to determine whether stocks were restricted or freely tradable. Oppenheimer also failed to conduct adequate supervisory reviews to determine whether the securities were registered. FINRA also found that Oppenheimer's AML programme did not focus on securities transactions and therefore, failed to monitor patterns of suspicious activity associated with the penny stock trades. In addition, Oppenheimer failed to conduct adequate due diligence on a correspondent account for a customer that was a broker-dealer in the Bahamas, and therefore a Foreign Financial Institution under the Bank Secrecy Act; the firm's failure contributed to Oppenheimer's failure to understand the nature of the customer's business and the anticipated

use of the account, which was to sell securities on behalf of parties not subject to Oppenheimer's AML review.

American Express

2013: Fine of US\$5.2mio¹⁸⁷

Agency: OFAC

The US Office of Foreign Assets Control ("OFAC"), fined American Express ("Amex") US\$5,226,120 because Amex's overseas offices booked travel to and from Cuba. OFAC justified the size of the fine due to a few aggravating factors such as (1) reckless disregard for the Cuba sanctions regulations, (2) knowledge by the company that the Cuba transactions "would or might take place," and (3) OFAC's provision of a notice in 1995 to Amex that the bookings were a violation of the Cuba sanctions. The fine related to long dated occurrences that no longer took place.

Guaranty Trust Bank

2013: £525,000 fine¹⁸⁸

Agency: UK Financial Conduct Authority (FCA) successor to FSA

The Financial Conduct Authority (FCA) has fined Guaranty Trust Bank (UK) Ltd (GT Bank) £525,000 for failings in its anti-money laundering (AML) controls for high risk customers between May 2008 and June 2010. These failings are particularly serious as they affected customers based in countries associated with a higher risk of money laundering, bribery or corruption, including accounts held by politically exposed persons (PEPs). The FCA's predecessor, the Financial Services Authority (FSA), reviewed GT Bank's controls as part of a thematic review into banks' management of money laundering risks in 2010. The review of GT Bank raised significant concerns and after further investigation, the FCA found that GT Bank failed to establish effective AML policies and procedures when they established their UK operations. This included failures to: i) assess or document potential money laundering risks posed by higher risk customers; ii) screen prospective customers against sanction lists or databases of PEPs; iii) obtain and/or document senior management approval to establish a business relationship with PEPs; iv) establish the purpose and intended nature of prospective customers' accounts or the sources of higher risk customers' wealth or funds; and v) review the activity of higher risk customers' accounts and check that the information they held on these customers was up to date. As a result, GT Bank was not able to fully understand or assess their higher risk customers' activities. This breached FCA Principle 3, which requires firms to take reasonable care to organise and control their affairs responsibly and effectively, and a number of FCA rules on systems and controls.

Tracey McDermott, director of enforcement and financial

crime, said: "Banks are at the front line in ensuring the proceeds of crime do not enter the UK financial system". GT Bank's failures were serious and systemic and resulted in an unacceptable risk of handling the proceeds of crime. "Regardless of whether firms are well established or new to the industry they must ensure that they have systems and controls to manage money laundering risk". GT Bank settled at an early stage of the investigation and qualified for a 30% discount on its fine. Without the discount the fine would have been £750,000.

According to the FCA Notice, GT Bank provided financial services to a significant number of higher risk customers, acting as a gateway to the UK financial system. However, 70% of these customers were based in countries which do not have requirements equivalent to those in the UK, and are recognised sources as posing a higher risk of money laundering. During the relevant period (May 2008 – June 2010) the FSA took action against a number of institutions for shortcomings in their financial crime systems and controls. As such, GT Bank should have been aware of the importance of systems and controls to prevent and detect all types of financial crime, including money laundering. As part of the settlement the regulator said that the bank had made a "strategic decision" to move away from establishing new relationships with PEPs and would, wherever possible, exit existing PEPs relationships. It has also significantly improved its compliance resourcing and its systems and controls. FCA investigators found that, in a sample of GT Bank's high-risk customer files, 46 out of 51 did not have adequate documentation to suggest that an AML review had taken place. The FCA said there was no evidence that the bank had properly considered all the potential risks for the customers. The FCA noted one example of a customer depositing a cheque for more than £500,000 from an offshore account into GT Bank. The bank failed to request any evidence about the source of the funds and how they were generated. It later emerged that the customer was wanted by the UK authorities in connection with the laundering of millions of dollars of embezzled public funds.

GT Bank also failed to record its screening results properly. The findings were only evidenced if there was a positive match, while in some instances customer screening had not been done before accounts were opened. In three cases accounts had been open for more than two years before being screened. The bank also failed to review its customers annually, as required, until July 2010. Forty-six of the 51 customer files reviewed by the FCA raised concerns about GT Bank's ongoing monitoring, the regulator said. Ade Adebisi, UK managing director GT Bank, said the failings happened during the bank's early years in the UK and that it had worked hard to ensure its systems were now fully compliant. "The FCA found no evidence that GTB UK did in fact handle any proceeds of crime. The total value

that passed through reviewed customer accounts was de minimis," he said.

JP Morgan Chase

2013: US\$410mio fine¹⁸⁹

Agency: Federal Energy Regulatory Commission (FERC)

JP Morgan Chase power-trading unit, JP Morgan Ventures Energy Corp manipulated electricity markets by misrepresenting the prices of electricity contracts with California and the Midwest that resulted in overpayments and fined US\$410mio by US electricity regulator, Federal Energy Regulatory Commission. This fine follows the one recently made with Barclays for US\$435mio and disxxxx at a further US\$34.9mio (see above). The fines are a sign of the increasingly aggressive stance taken by FERC, a relatively speaking low-profile federal agency that oversees transmission lines, natural-gas pipelines and power trading markets across the US. Using enforcement muscle beefed up in the wake of Enron Corp's collapse, the agency is broadly scrutinizing potential manipulation of energy markets and has sought fines from Wall Street firms that include Barclays (see above) and Deutsche Bank which also settled with FERC. Many of the biggest US banks and trading firms began buying and selling power in the US's deregulated energy markets following a California Energy Crisis in 2001, which was caused in part by manipulative trading behavior linked to Enron. Following Enron's collapse, FERC received authority from Congress to levy fines of up to US\$1mio per violation per day, up from US\$10,000 per violation. It has assessed US\$291mio in penalties since 2007 in 78 separate enforcement actions. JP Morgan began buying and selling energy largely because of its 2008 purchase of securities firm Bear Stearns Co, which had a power group based in Houston. It is alleged that the manipulation occurred as follows: traders would submit a relatively low bid to deliver electricity in the "day-ahead" market, ensuring that system operators would schedule their power plant to turn on the following day. Then the traders would make an offer the next day to deliver electricity from that same plant at a relatively high price, which prevented them from being chosen to provide electricity that day. While the traders might lose money because they were not dispatched to generate power, they would also be eligible for a "make-whole" payment because their power plant unit had been scheduled the day ahead to deliver a substantial amount of electricity. The "make-whole" payment could cover any losses and generate a profit for the firm overall. JP Morgan will pay US\$124mio to California residents who overpaid for electricity. Customers in the midwest will receive US\$1mio. The rest of the fine is to be paid to the US Treasury.

JP Morgan Chase

2013: US\$1.020bio¹⁹⁰

Agencies: US SEC; OCC; FED; UK FCA

JP Morgan Chase agreed to pay US\$1.020mio in fines stemming from its 2012 “London Whale” incident, which amount to one of the largest ever levied against a bank over a single trading strategy. The money will go to the US Securities and Exchange Commission, (US\$200mio), the Office of the Comptroller of the Currency, (US\$300mio), the Federal Reserve, (US\$200mio), the Commodity Futures Trading Commission (US\$100mio) and Britain’s Financial Conduct Authority, (US\$220mio/ £137.6mio). As part of the settlement, the bank will also admit wrongdoing and acknowledge that lax internal controls were partly responsible for allowing the massive derivative wagers made by traders in the London office that ultimately cost the bank more than US6bio in losses. These are settlements of civil actions against JP Morgan Chase who may still face the FBI and federal prosecutors who are still considering criminal investigations.

Saddle River Valley Bank

2013: US\$8.2mio¹⁹¹

Agencies: OCC and FINCEN

The Saddle River Valley Bank (SRVB) was fined US\$8.2mio by the OCC and FINCEN for violation of US money laundering laws and regulations. Beginning at least as early as 2000, numerous federal agencies, including the Department of State, the Department of the Treasury, the Federal Reserve Bank, and the IRS, began issuing public warnings to US financial institutions about the increased money laundering threat present in Mexico. These warnings were also available through industry-wide advisories. It was believed that the proceeds of narcotics sales in the US were being disproportionately laundered and transferred through banking institutions in Mexico. Many of these warnings also discussed the specific money laundering risks associated with “Casas de Cambio,” (CDCs), which are non-bank currency exchange businesses located in Mexico and elsewhere.

Beginning in June 2009, SRVB began servicing what would ultimately become four CDCs, including three CDCs in Mexico and one in the Dominican Republic. SRVB voluntarily severed its relationship with the CDCs by May 2011 but only after processing at least US\$1.5bio in transactions on behalf of the CDCs. SRVB’s anti-money laundering programme related to the CDCs was deficient in several key areas, in particular SRVB failed to: appropriately monitor at least US\$1.5bio in transactions conducted on behalf of the CDCs; properly detect and report suspicious activity occurring within the CDC accounts and file Suspicious Activity Reports on a timely basis; conduct sufficient enhanced due diligence on the CDCs; have a BSA officer or other

personnel with sufficient experience to operate an AML programme; provide adequate training to its employees concerning anti-money laundering and retain qualified periodic independent testers for its anti-money laundering programme, as required by the BSA. After a joint investigation by the US Attorney’s Office for the District of New Jersey and the OCC, SRVB agreed to an assessed civil monetary penalty by the OCC of US\$4.1mio for the deficiencies in its anti-money laundering programme. SRVB has agreed to a concurrent civil monetary penalty by FinCEN of US\$4.1mio, to be satisfied by one payment to the U.S. Treasury Department on behalf of both actions by the OCC and FinCEN. SRVB also agreed to surrender and forfeit an additional US\$4.1mio to the US to resolve the investigation conducted by the US Attorney’s Office for the District of New Jersey and the OCC, for a total penalty of US\$8.2mio.

TCF National Bank

2013: US\$10mio CMP¹⁹²

Agency: OCC

TCF National Bank, based in Sioux Falls, South Dakota was fined US\$10mio by the OCC for violations of the Bank Secrecy Act (BSA). An OCC examination of the bank’s account and transaction activity between November 2008 and July 2010 revealed late filing of suspicious activity reports (SARs). The suspicious activities primarily consisted of cash transactions which indicated structuring and wire transfers where the source and purpose of the funds were unknown. In addition, upon further investigation, the OCC found instances where SARs failed to adequately explain or identify potential terrorist financing. The CMP follows a cease and desist order issued in July 2010 which directed the bank to correct deficiencies in its BSA and anti-money laundering programmes and required an independent examination of BSA reports filed between November 2008 and July 2010.

TD Bank

2013: US\$5.25mio (US\$37.5mio CMP - and US\$15mio)¹⁹³

Agencies: FINCEN/ OCC - SEC

TD Bank, N.A. was fined US\$37.5mio by the US Financial Crimes Enforcement Network (FinCEN) and the OCC for failures in filing suspicious activity reports related to the Ponzi scheme orchestrated by Florida attorney Scott Rothstein. Additionally, the Securities and Exchange Commission has assessed a separate US\$15mio penalty against the Bank for related securities violations.

From April 2008 through September 2009, the Bank was found to have wilfully violated the Bank Secrecy Act’s reporting requirements by failing to detect and adequately

report suspicious activities in a timely manner. During that period, Rothstein orchestrated a major Ponzi scheme by fraudulently inducing victims to invest in purported settlements involving whistleblower and sexual harassment lawsuits. Thousands of transactions flowed through his multiple law firm accounts at TD Bank which included transactions related to Rothstein’s Ponzi scheme. While the Rothstein law firm’s accounts alerted in TD Bank’s anti-money laundering surveillance software for suspicious activity, TD Bank employees failed to recognise the suspicious activity and file SARs in a timely manner. In 2010, Rothstein pleaded guilty to a racketeering conspiracy in the US District Court for the Southern District of Florida and is currently serving a 50-year prison sentence.

In 2011, the Bank conducted a review of the Rothstein transactions. Based on the results of the review it filed five late suspicious activity reports, totaling an estimated US\$900mio in aggregate suspicious transaction activity occurring between April 2008 and October 2009. A lack of adequate training for both the anti-money laundering and business staff contributed to the failure to recognise this suspicious activity.

“In the face of repeated alerts on Mr. Rothstein’s accounts by the Bank’s anti-money laundering surveillance software over an 18 month period, the Bank did not do enough to prevent the pain and financial suffering of innocent investors,” FinCEN Director Jennifer Shasky Calvery stated. “Financial institutions must do a better job of protecting our financial system and citizens from such harm. It is not acceptable to have a poorly resourced and trained staff overseeing such a critical function.”

Indian Banks

2013: US\$1mio¹⁹⁴

Agency: Reserve Bank of India

The Reserve Bank of India imposed fines in aggregate of just over US\$1mio on six Indian banks for violation of the Reserve Bank of India Know Your Customer/Anti-Money Laundering Standards, following industry wide inspections during April and May 2013. The Banks and respective fines involved the following: Allahabad Bank (Rs. 0.50 Crore ~ US\$78K); Bank of Maharashtra (Rs. 0.501 Crore ~ US\$78K); Corporation Bank (Rs. 1.50 Crore ~ US\$233K); Dena Bank (Rs. 2.00 Crore ~ US\$311K); IDBI Bank Ltd. (Rs. 1Cr ~ US\$155K) and Indian Bank (Rs. 1Cr ~ US\$155K). The violations ranged across the AML environment including with respect to the non-adherence to certain aspects of know your customer (KYC) norms and anti-money laundering (AML) guidelines like customer identification procedure, risk categorisation, periodical review of risk profiling of account holders, periodical KYC updates, non-adherence of KYC norms for walk in customers

including for sale of third party products, omissions in filing of cash transaction reports (CTRs) in respect of some cash transactions, non-adherence to instructions on monitoring of transactions in customer accounts including walk-in-customers, non-adherence to instructions which prohibit acceptance of cash above Rs50,000 from customers for sale of gold coins and issue of demand drafts, non-adherence to instructions on import of gold on consignment basis and non-adherence to instructions on permitted credits to Non-resident accounts. The investigation did not reveal any *prima facie* evidence of actual money laundering.

Swiss Bank Fines

2013: US\$216,000 (HSBC; UBP; EFG)¹⁹⁵

Agency: Swiss FINMA

Three Swiss banks were ordered to pay fines up to CHF100,000 for handling suspicious funds from friends and relatives of Tunisia’s ousted President Ben-Ali. President Zine al-Abidine Ben Ali, who ruled for 23 years, fled Tunisia in 2011 after popular protests against his regime. HSBC Private Bank, Union Bancaire Privee (UBP) and EFG were fined by the Financial Market Supervisory Authority for mismanaging funds from those in the President’s regime.

According to press reports, HSBC Private Bank, received the most severe punishment, receiving a fine of 88,000 CHF (US\$98,000) and have installed an external auditor and had imposed a ban on opening accounts for politically exposed persons (PEPs) for three years. In an aim to curtail money laundering and other criminal activity Swiss law dictates that banks must pay close attention to those holding high offices in government (PEPs) and their family members. EFG was fined 46,000 Swiss francs (CHF) (US\$51,000) and UBP fined 49,000 CHF (US\$57,000). These actions and fines result from an investigation carried out by FINMA the Swiss market regulator, following the Arab Spring. It had been announced initially that 20 Banks were being reviewed and that 4 Banks are likely to face measures. The 3 announced relate solely to Tunisian assets so it could be expected that further announcement with respect to either Libya or Egyptian assets could follow.

Royal Bank of Scotland

2013 - US\$100mio CMP Cease and Desist¹⁹⁶

Agencies: US FED; OFAC; DFS

UK based Bank, Royal Bank of Scotland Group agreed to pay US\$100mio in penalties to settle allegations by US regulators that the bank violated US sanctions against Iran, Sudan, Burma and Cuba. This includes a Cease and Desist Order and a payment of US\$50mio to the Fed, of which US\$33mio is deemed to satisfy an OFAC penalty, with another US\$50mio to the New York State Department of Financial Services (DFS). The US Department of Justice

and the District Attorney of New York have concluded their parallel criminal investigations and have decided not to take any action against RBS.

From 2005 to 2009, RBS is alleged to have engaged in payment practices that interfered with the implementation of US economic sanctions by financial institutions in the US. Those practices included removing material references to US-sanctioned locations or persons from payment messages sent to U.S. financial institutions. The DFS said that between 2002 and 2011 RBS hid or failed to disclose information about sanctioned parties in 3,500 transactions valued at approximately US\$523mio. The DFS noted that employees at RBS acted to conceal the identity of sanctioned clients by various means, including implementing formal procedures to strip out identifying data from payment messages. According to US regulators, with respect to Iran, RBS developed written procedures to send payments that omitted information about the Iranian nexus in cover payments sent to US financial institutions. The procedures instructed RBS employees to list the actual name of the Iranian financial institution rather than the Bank Identifier Code in the beneficiary bank field of the payment instructions.

The US Department of the Treasury said in a statement, "Doing so prevented the RBS payment system from automatically including references to the Iranian bank or Iran in related cover messages and resulted in the omission of that data from instructions sent to US clearing banks. While the instructions were developed to handle payments involving Iran, RBS identified that similar methods were used for certain payments involving Sudan, Burma, and Cuba as well."

According to RBS, the settlement arose from an investigation initiated by the bank in 2010 into its historical US dollar payment practices and controls in the UK and that the review was shared by it with the relevant US authorities in 2010.

RBS announced that it had embarked on an extensive remediation plan to address the shortcomings identified in its investigation, including committing almost £300 million (since 2010) to strengthen the bank's control environment on sanctions, and since 2009, RBS has instituted a new more comprehensive global OFAC compliance policy, the introduction of electronic filtering of payments including an enhanced filtering approach, conducted an extensive review of all customer relationships in the relevant countries and exited a number of customer relationships, enhanced its Anti-Money Laundering and Sanctions Compliance function and increased its team by more than 730 employees since June 2011 to a total of 1,700 today. It also strengthened governance at a number of different levels within the Group to ensure the appropriate coordination and prioritization of sanctions compliance activity across the Group.

JLT Specialty

2013: £1.8 mio¹⁹⁷

Agency: UK Financial Conduct Authority

JLT Specialty provides insurance, broking, risk management and claims consulting services to a wide range of national and international corporate clients, but in so doing the FCA found that the Company had failed to implement adequate risk management systems and controls over anti bribery and corruption, including weaknesses around due diligence on overseas introducer's and generally failing to implement issued policies and procedures, in particular red flag areas identified as warranting greater attention in the firms own policies and procedures.

Outlook Cases/2014 and beyond

Without prejudging outcomes in any way, the following have been publicly disclosed and so are mentioned as a matter of record and for information only. No conclusions can be made until facts and findings if any are revealed.

Sanctions

According to press reports and in some cases confirmed by the Bank itself the following Financial Institutions are co-operating with US investigations into possible breaches of US Sanctions. The Banks are thought to include Unicredit's German subsidiary, **HypoVereinsbank**, which the Italian bank bought in 2005, other German Banks; **Commerzbank** and **Deutsche Bank** and French Banks' **BNP Paribas** and **Credit Agricole**.

The UK authorities in 2011 concluded and published findings from a thematic review, which focused on how banks manage money laundering risk in higher risk situations, uncovering in their words "serious weaknesses" in some banks' systems and controls and finding that three quarters of institutions were managing their money laundering risks inadequately. The majority of these failings were related to the handling of PEPs. Since then the FSA and its successor the FCA has fined Swiss bank **EFG Private Bank** £4.2mio, **Coutts** £8.75mio and **Habib Bank** was fined £525,000, while its money laundering reporting officer was fined £17,500. The recent fine for **GT Bank** of £525,000 brings the list of offenders to 4 with one more unnamed institution thought to still face censure resulting from the regulator's thematic review, thought to be **Standard Bank** (see below)

Libor

According to the WSJ,^{198/199} regulators hope to reach settlements with others, including **Lloyds**, **Bank of America**, **Citigroup** and **JPMorgan Chase** as well as **Deutsche Bank**. Other reports also name **HSBC**. The EU Commission are still investigating **HSBC**, **JP Morgan**, **Credit Agricole** and **ICAP**.

Cross Border Tax Cases

According to media reports^{200/201} a number of Banks are under investigation/ co-operating in connection with probes by US authorities investigating tax matters, including Banks in Switzerland, namely **Credit Suisse**, **Julius Baer**, **Pictet & Cie**, the **Zürcher and Basler Kantonal Banks**, **Bank Frey**, **HSBC**'s Swiss subsidiary and Israel's **Bank Leumi**. **Credit Suisse** had previously announced it was making a provision of CH250mio. These 8 banks are likely not the only ones with 6 more expected to make 14. In August 2013 the US

and Swiss governments announced a framework for co-operation which would not include the 14 banks still under criminal investigation. Instead it will apply to Switzerland's 2nd tier of around 100 banks, which will be divided up into 3 groups, with fines expected to range from 20-50% of the total amount of hidden US assets in Swiss accounts up to August 2008. Eligible banks will pay penalties and disclose account information about US customers in order to avoid prosecution. The Chairman of the Swiss Bankers Association, Patrick Odier, commented that "the situation would be sorted out within the next 12-18 months" but also offered an apology, stating "it was not because we lacked skills and knowledge that we found ourselves in these unfortunate situations....it was because we acted wrongly and we displayed wrong conduct".

Others

Barclays has said that UK and US authorities have opened an investigation into how the Bank raised money from Middle Eastern investors during the first phase of the financial crisis. According to press reports^{202/203} the probes relate to both the granting of a banking license in Saudi Arabia as well as capital raising and dealings in Qatar. The bank turned to the Qatar Investment Authority for two capital raisings in 2008. Barclays disclosed that year that £300mio had been paid in fees and commissions as part of the deal, including £66mio to Qatar Holding "for having arranged certain of the subscriptions in the capital raising".

JP Morgan Chase have acknowledged being the subject of an SEC investigation into the Bank's hiring practices. According to reports the SEC and the US Justice Department are trying to determine whether the Bank's hiring practices violated US anti-bribery laws. The focus on the hiring of so-called "princelings" was sparked after the US government began looking into hires that could have helped the Bank (and others) win lucrative IPOs in the region.²⁰⁴

The SEC charged the former head of the Miami office at brokerage firm **Direct Access Partners ("DAP")** for his role in an alleged kickback scheme to secure the bond trading business of Bandes, a state-owned Venezuelan bank. The SEC previously charged four individuals who enabled the global markets group at DAP to generate more than US\$66mio in revenue from transaction fees related to fraudulent trades they executed for Bandes. A portion of this revenue was illicitly paid to the Vice President of Finance at Bandes, who authorised the fraudulent trades. According to the SEC, the managing partner and others executed internal wash trades, interpositioned another broker-dealer in the trades to conceal their role in the transactions, and engaged in massive round-trip trades to pad their revenue. The SEC's amended complaint charges the managing partner and the other defendants with fraud.²⁰⁵

Breaking News

Brief Update from start of the Year to end March 2014.

As this book was finalised at the end of December 2013 and intended to be up to date as at this date, the Author will issue quarterly updates, including brief summaries of the most important quarterly developments, the first of which is set out below covering the period from the start of the year to the end of March 2014.

Part 1 Section 1 Predicate Crimes

Bribery & Corruption

The EU issued its first ever Anti-Corruption Report¹ which covered all 28 EU Member States, concluding that Corruption continues to be a challenge for Europe, with corruption costs for the European economy estimated at around €120 billion per year. The report shows that both the nature and level of corruption, and the effectiveness of measures taken to fight it, vary from one Member State to another. It also shows that corruption deserves greater attention in all Member States. The Report also publishes the results of a survey which found that three quarters (76%) of Europeans think that corruption is widespread and more than half (56%) think that the level of corruption in their country has increased over the past three years. One out of twelve Europeans (8%) say they have experienced or witnessed a case of corruption in the past year. The Report believes that there are great differences in many Member States due to the approaches taken, with for some, effective prevention contributing to a strong reputation of little corruption, whereas others have implemented policies in an uneven way and with limited results. Conflicts of interests were highlighted, differences as to the likelihood of prosecution and the severity of punishment another area identified. Risk areas include politics, with integrity in politics an issue still for many Member States and in particular the risks are generally higher at regional and local levels, where checks and balances and internal controls tend to be weaker, than at the central level. Urban development and construction, as well as health care, are sectors identified as vulnerable to corruption in a number of Member States, as well as shortcomings regarding the supervision of state-owned companies, increasing their vulnerability to corruption. Public procurement is also an area identified as vulnerable to corruption as approximately one fifth of the EU's GDP is spent every year by public entities buying goods, works and services.

Fraud including Tax Fraud & Cybercrime

The British Bankers Association (BBA) warned its members about cyber-attacks and the dangers posed but also about their responsibilities and in particular information sharing and reporting obligations in such a case, this following the publication of the Bank of England's findings of the "war game exercise" conducted in November 2013 known as "Waking Shark II." The

Report² has provided important lessons to both Industry and Government, with the need to use an available protected common platform for reporting and information sharing during potential stress scenarios and the need to not only inform Regulators and share important information with other market participants, in order to gauge, understand and respond to a market threat but also to inform Law Enforcement and file Suspicious Activity Reports.

Part 1 Section 2 Sub-Section 4 Country Risks

The FATF Plenary held in Paris in February 2014 published updates to its list of Countries with strategic anti-money laundering and combating the financing of terrorism (AML/CFT) deficiencies. FATF cited the following Countries with Iran and North Korea still requiring counter-measures, the others with strategic deficiencies being: Algeria, Ecuador, Ethiopia, Indonesia, Myanmar, Pakistan, Syria, Turkey, Yemen, followed by Countries with strategic AML/CFT deficiencies for which they have developed an action plan with the FATF, being: Albania, Angola, Argentina, Cuba, Iraq, Kenya, Kuwait, Kyrgyzstan, Lao PDR, Mongolia, Namibia, Nepal, Nicaragua, Papua New Guinea, Sudan, Tajikistan, Tanzania, Uganda, Zimbabwe. In this group Countries not making sufficient progress were identified as Afghanistan and Cambodia. FATF also received an update on AML/CFT improvements in Antigua and Barbuda, Bangladesh and Vietnam, which allowed these last 3 countries to be removed from the above list.

Part 1 Section 4 Laws & Regulations

AML Treaties, Conventions & Major Laws

The Consultative Paper from the Basel Committee on Banking Supervision, titled, "Sound Management of Risks related to money laundering and the financing of terrorism" was issued in final form.³

Financial Action Task Force

FATF work in 2014

The FATF Plenary held in Paris in February 2014 under the Russian Presidency published updates to its list of Countries with strategic anti-money laundering and combating the financing of terrorism (AML/CFT) deficiencies (see above). FATF also approved and published follow-up reports to the mutual evaluations of Aruba (Kingdom of the Netherlands), Austria, Canada, Luxembourg, Mexico and the Netherlands. Finally FATF reviewed the voluntary tax compliance programmes in several jurisdictions, adopted and published universal procedures for assessments conducted by assessment bodies, continued to develop guidance on effective implementation of beneficial ownership requirements, explored common issues between AML/CFT and data protection experts and is conducting further research on the AML/CFT implications of virtual currencies.

The Wolfsberg Group

In response to increasing regulatory focus on the risks associated with Correspondent Banking, The Wolfsberg Group announced revised Anti-Money Laundering Principles for Correspondent Banking, Frequently Asked Questions on Correspondent Banking and Wolfsberg Group Anti-Money Laundering Questionnaire. The Wolfsberg Group also announced the publication of its Guidance Paper on Mobile and Internet Payment Services (MIPS). Addressing the growing demand in the marketplace, and in financial institutions, for migration from paper based payments to MIPS, the paper considers the money laundering risks and mitigants of MIPS and supplements the Wolfsberg Group Statements on Credit/Charge Card Issuing and Merchant Acquiring Activities and Prepaid and Stored Value Cards. The paper seeks to counter the widely-held perception that all MIPS arrangements represent automatic high risk of money laundering by underlining that there is a broad spectrum of risk and mitigants for these arrangements.

Sanctions & Embargoes

Developments with Iran have slightly improved with an initial agreement to explore talks under the Joint Plan of Action ("JPA"), between Iran and the P5+1 countries (China, France, Germany, the Russian Federation, the UK and the US) which led to the temporary lifting of certain Iran-related sanctions. These sanctions suspensions became effective on January 20, 2014, and are mostly related to activity involving non-US persons and activity involving transactions relating to Iran's exports of petrochemical products, precious metals and transactions involving the automotive sector. Dealings involving US products/US persons involving medicines, medical supplies, food and agricultural related products, may also be permissible under general licenses issued by the US Treasury Department. This temporary lifting of sanctions by the US, however, does not include investments in Iran. Except in limited circumstances, US persons continue to be subject to sanctions against Iran and any Iranian designated party under sanctions issued by the US Treasury Department and enforced by the Office of Foreign Assets Control (OFAC), and the US Department of State which imposes restrictions with regards to exports of US goods directly or indirectly to Iran. The US also lifted certain "secondary" sanctions against non-US persons engaged in activity with Iran. The JPA is due to expire July 20, 2014 and the US has made clear that if a permanent deal with Iran is not reached, all sanctions, including sanctions against non-US persons, will be re-instated. Any dealings with Iran that are permissible as a result of the lifting of sanctions must be concluded on or before July 20, 2014. There will be no grandfathering of business dealings that are not completed by that date. There is no certainty that a long term agreement with Iran will be reached that could extend this temporary sanctions relief. In response to the JPA, third Countries have also acted including for example, Switzerland that lifted a ban on precious metal trading with Iranian public entities and eased restrictions on trading in petrochemical products,

transport of Iranian oil and petroleum products and insurance transactions relating to shipping until August 2014. Switzerland also increased the ceiling for transfers of funds to Iranian nationals.

The EU and the US imposed sanctions on more than two dozen Russian and Ukrainian officials following the crises in the Ukraine and Russian attempts to annex Crimea and threatened more severe moves if Moscow continues. Washington targeted seven top Russian policy makers including some of President Vladimir Putin's closest advisers with asset freezes and travel bans and the EU took measures against 21 people, including 13 Russians. The seven Russians hit by US sanctions include Vladislav Surkov and Sergei Glaziev, two aides to Mr Putin; Dmitry Rogozin, a deputy prime minister, and Valentina Matviyenko, head of the Federation Council, or upper house of parliament. Washington also placed sanctions on Sergei Aksyonov, the new pro-Russian prime minister of Crimea, and Vladimir Konstantinov, speaker of the Crimean parliament. The White House said its "current focus" was on targeting particular individuals and their personal assets "but not companies that they may manage on behalf of the Russian state". However, the US order also allows Washington to impose curbs on "any individual or entity that operates in the Russian arms industry". The 21 officials targeted by EU sanctions also includes people from Russia's parliament and armed forces but not Mr Putin's immediate circle.

Part 2 Section 5 Regions, Countries, Criminals & Terrorists

Following the election of less hardline Iranian President Hassan Rouhani in 2013, talks ensued and an interim agreement, the so called Joint Plan of Action ("JPA")), between Iran and the P5+1 countries (China, France, Germany, the Russian Federation, the UK and the US) came into force in January 2014. For details on the temporary lifting of certain Sanctions and Embargoes see above.

Major developments in this period focussed on the continuing instability and political unrest in the Ukraine, where with protesters increasingly active, particularly in Western Ukraine and in Kiev, its Capital, the government of President Yanukovic fell, with the President fleeing first to the East and now residing in Moscow. With a new interim government installed under acting President Oleksander Turchinov, the former Parliamentary speaker, an immediate crisis ensued with the Eastern Region of Crimea, which is home to a majority of former Russians, coming under direct Russian control followed by a vote in Crimea first by the Crimean Parliament and then by a hastily Organised Referendum to leave Ukraine and to join Russia. As at the time of writing and with the crises continuing Sanctions first against former Ukrainian officials and against targeted Russian persons have been the initial Western response (US/EU). For more details on Sanctions & Embargoes

see above. Whilst going into this quarter most eyes were on the Winter Olympics held in the Russian City of Sochi, with fears of terrorist acts from the Caucasus Emirate of most concern, the security arrangements may have deterred attacks and the games thankfully passed off without incident. With the games just at an end and Russia seeking to promote itself in a new light towards the world and after spending amounts up to US\$30 bio, for this purpose, the aggressive acts in the Crimea have not only tarnished that image but set back Russia's ability to act as a reliable partner on the International stage.

Part 2 Section 6 Terrorist Attacks

2014: Terrorist Attack at Train Station in Kunming, China by Xinjiang extremists (29)

At least 29 people died and 140 were injured in an orchestrated knife attack, at a Chinese Railway Station in Kunming which Chinese state media have called "China's September 11th". Chinese authorities say it was an act of terrorism carried out by "Xinjiang extremists", or ethnic Uighurs, a Muslim minority group from the north-west, perhaps carried out by members of the East Turkستان Islamic Movement.

Numerous attacks by Boko Haram in Nigeria (700)

According to Human Rights Watch the killings in Nigeria by Boko Haram have intensified in 2014. With more than 40 significant attacks so far, the death toll has reached 700 people.

Part 2 Section 8 Enforcement Cases

JP Morgan Chase

2014: US\$2.05bio (US\$1.7 bio forfeiture for investors/US\$350mio OCC (US\$461 mio FINCEN)⁴
Agencies: US DoJ & OCC & FINCEN

Five years after Bernie Madoff admitted to operating the largest ever Ponzi scheme, Madoff's custodian bank, JPMorgan Chase (JPM) agreed to two criminal violations of the Bank Secrecy Act tied to its relationship as Madoff's primary banker for over two decades as authorities believe the company ignored signs of the fraud. JPM agreed to pay US\$1.7 billion to victims of the Madoff fraud and agreed to reform its anti-money laundering policies, paying a fine levied by the OCC of US\$350mio. The deal with U.S. authorities includes a two-year deferred prosecution agreement and represents the largest-ever bank forfeiture in the U.S. and largest ever combined forfeiture and fine for money laundering related matters. JPM agreed to overhaul and reform its anti-money laundering policies, after the OCC found "critical and widespread deficiencies" of the bank's anti-money laundering compliance programs. The OCC said the penalty is based on JPMorgan's failure to report suspicions about Madoff's investment firm to U.S. law enforcement and regulators despite alerting U.K. authorities. Concurrent with the OCC's enforcement action, the Financial Crimes Enforcement Network assessed

a US\$461 million civil money penalty that is deemed satisfied by the forfeiture to the U.S. government.

Standard Bank

2014: £7,640,400⁵

Agency: The UK Financial Conduct Authority

The UK financial Conduct Authority (FCA) fined Standard Bank PLC (Standard Bank PLC is the UK subsidiary of Standard Bank Group, South Africa's largest banking group) £7,640,400 for failings relating to its anti-money laundering (AML) policies and procedures over corporate customers connected to politically exposed persons (PEPs). This action flows from the 2011 published review by the FSA in connection with an undertaken thematic review, which focused on how banks manage money laundering risk in higher risk situations. Tracey McDermott, director of enforcement and financial crime, said: "One of the FCA's objectives is to protect and enhance the integrity of the UK financial system. Banks are in the front line in the fight against money laundering. If they accept business from high risk customers they must have effective systems, controls and practices in place to manage that risk. Standard Bank clearly failed in this respect."

Canada Inc formerly Swift Trade Inc

2014: £8,000,000⁶

Agency: The UK Financial Conduct Authority

The Financial Conduct Authority (FCA) issued a Final Notice against Canada Inc formerly carrying on business as Swift Trade Inc ("Swift Trade") and levied a financial penalty of £8,000,000 for engaging in market abuse.

Credit Suisse

2014: US\$196 mio Fine⁷

Agency: The Securities and Exchange Commission

Credit Suisse Group AG was fined for violating federal securities laws by providing cross-border brokerage and investment advisory services to US clients without first registering with the SEC. Credit Suisse agreed to pay US\$196mio and admit wrongdoing to settle the SEC's charges. According to the SEC's order instituting settled administrative proceedings, Credit Suisse provided cross-border securities services to thousands of US clients and collected fees totaling approximately US\$82mio without adhering to the registration provisions of the federal securities laws. Credit Suisse relationship managers traveled to the US to solicit clients, provide investment advice, and induce securities transactions. These relationship managers were not registered to provide brokerage or advisory services, nor were they affiliated with a registered entity. The relationship managers also communicated with clients in the US through overseas e-mails and phone calls. "The broker-dealer and investment adviser registration provisions are core protections for investors," said Andrew J. Ceresney, director

of the SEC's Division of Enforcement. "As Credit Suisse admitted as part of the settlement, its employees for many years failed to comply with these requirements, and the firm took far too long to achieve compliance." According to the SEC's order, Credit Suisse began conducting cross-border advisory and brokerage services for US clients as early as 2002, amassing as many as 8,500 US client accounts that contained an average total of US\$5.6bion in securities assets. The relationship managers made approximately 107 trips to the US during a seven-year period and provided broker-dealer and advisory services to hundreds of clients they visited. Credit Suisse was aware of the registration requirements of the federal securities laws and undertook initiatives designed to prevent such violations. These initiatives largely failed, however, because they were not effectively implemented or monitored. According to the SEC's order, it was not until after a much-publicised civil and criminal investigation into similar conduct by Swiss-based UBS that Credit Suisse began to take steps in October 2008 to exit the business of providing cross-border advisory and brokerage services to US clients. Although the number of US client accounts decreased beginning in 2009 and the majority were closed or transferred by 2010, it took Credit Suisse until mid-2013 to completely exit the cross-border business as the firm continued to collect broker-dealer and investment adviser fees on some accounts. The SEC's order finds that Credit Suisse willfully violated Section 15(a) of the Securities Exchange Act of 1934 and Section 203(a) of the Investment Advisers Act of 1940. Credit Suisse admitted the facts in the SEC's order acknowledged that its conduct violated the federal securities laws, accepted a censure and a cease-and-desist order and agreed to retain an independent consultant. Credit Suisse agreed to pay US\$82,170,990 in disgorgement, US\$64,340,024 in pre-judgment interest, and a US\$50mio penalty.

Whilst the settlement with the SEC closes one important aspect of US investigations into Credit Suisse's cross-border US business, the Bank still has likely larger fines and agreements still to reach with the US Department of Justice and the US IRS, particularly to answer allegations contained in a Report issued by the US Senate on Permanent Investigations, entitled: Offshore Tax Evasion: The Effort to Collect Unpaid Taxes on Billions in Hidden Offshore Accounts and discussed in Hearings held in February 2014.⁸ After paying US\$196mio fine, Credit Suisse still has a disclosed reserve of around CHF300mio set aside for further fines and penalties, though many commentators believe the final figure is more likely to surpass the US\$780mio paid by UBS in 2009. As a result of the findings from tax investigations such as this, the US Congress enacted the Foreign Account Tax Compliance Act, requiring banks to disclose American customer accounts every year or pay a 30% tax on their US investment income. But there are loopholes in the law that, among other things, allow foreign financial firms to protect US offshore shell companies.

Gold Fixing Investigation

The London gold fix, the benchmark used by miners, jewellers and central banks to value the metal, may have been manipulated for a decade by the banks setting it, and is the subject of continued investigations by Regulators. With an estimated 175m ounces of gold, worth US\$215bn at today's prices, changing hands daily on the over-the-counter market, London is the global centre of gold trading. Unusual trading patterns around 3 p.m. in London, when the so-called afternoon fix is set on a private conference call between five of the biggest gold dealers, may be a sign of collusive behavior. The rate-setting ritual dates back to 1919. Dealers in the early years met in a wood-paneled room in Rothschild's office in the City of London and raised little Union Jacks to indicate interest. Now the fix is calculated twice a day on telephone conferences at 10:30 a.m. and 3 p.m. London time. The calls usually last 10 minutes, though they can run more than an hour. The five Banks overseeing the century-old rate are until recently Barclays, Deutsche, Bank of Nova Scotia, HSBC and Société Générale, though Deutsche Bank have recently announced their intention to withdraw from the Gold fixing. Deutsche have also announced withdrawing from the Silver fixing which is carried out with two other Banks, HSBC and Scotiabank and is fixed in a similar way to the Gold price.

Brown Brothers Harriman & Co

2014: US\$8mio⁹

Agency: FINRA

FINRA Fined Brown Brothers Harriman a Record US\$8 Million for Substantial Anti-Money Laundering Compliance Failures and fined and suspended a former AML Compliance Officer in particular over BBH's failure to have an adequate anti-money laundering program in place to monitor and detect suspicious penny stock transactions. BBH also failed to sufficiently investigate potentially suspicious penny stock activity brought to the firm's attention and did not fulfill its Suspicious Activity Report (SAR) filing requirements. In addition, BBH did not have an adequate supervisory system to prevent the distribution of unregistered securities. BBH's former Global AML Compliance Officer Harold Crawford was also fined US\$25,000 and suspended for one month.

Penny stock transactions pose heightened risks because low-priced securities may be manipulated by fraudsters. FINRA found that from 1 January 2009, to 30 June 2013, BBH executed transactions or delivered securities involving at least six billion shares of penny stocks, many on behalf of undisclosed customers of foreign banks in known bank secrecy havens. BBH executed these transactions despite the fact that it was unable to obtain information essential to verify that the stocks were free trading. In many instances, BBH lacked such basic information as the identity of the stock's beneficial owner, the circumstances under which the stock

was obtained, and the seller's relationship to the issuer. Penny stock transactions generated at least US\$850mio in proceeds for BBH's customers.

Brad Bennett, FINRA Executive Vice President, Enforcement, said "The sanction in this case reflects the gravity of Brown Brothers Harriman's compliance failures. The firm opened its doors to undisclosed sellers of penny stocks from secrecy havens without regard for who was behind those transactions, or whether the stock was properly registered or exempt from registration. This case is a reminder to firms of what can happen if they choose to engage in the penny stock liquidation business when they lack the ability to manage the risks involved."

FINRA also found that although BBH was aware that customers were depositing and selling large blocks of penny stocks, it failed to ensure that its supervisory reviews were adequate to determine whether the securities were part of an illegal unregistered distribution. FINRA Regulatory Notice 09-05 discusses "red flags" that should signal a firm to closely scrutinize transactions to determine whether the stock is properly registered or exempt from registration, or whether it is being offered illegally. BBH customers deposited and sold penny stock shares in transactions that should have raised numerous red flags.

In concluding these settlements, BBH and Crawford neither admitted nor denied the charges, but consented to the entry of FINRA's findings.

Forex Probe

The forex probe is a financial investigation into whether the world's largest currency trading banks colluded to manipulate the daily foreign exchange rates.¹⁰ Market regulators in Asia, Switzerland, the UK and the US began to investigate the US\$5.3 trillion-a-day foreign-exchange market after Bloomberg News reported in June 2013 that currency dealers said they had been front-running client orders and rigging the foreign exchange benchmark WM/Reuters rates by colluding with counterparts and pushing through trades before and during the 60-second windows when the benchmark rates are set. The behavior occurred daily in the spot foreign-exchange market and went on for at least a decade according to currency traders using electronic chatrooms in which senior currency traders discussed with their competitors at other banks the types and volume of the trades they planned to place. The electronic chatrooms had names such as "The Cartel," "The Bandits' Club," "One Team, One Dream" and "The Mafia". At least 15 banks including Barclays, HSBC and Goldman Sachs disclosed investigations by regulators. Barclays, Citigroup, and JPMorgan Chase all suspended or placed on leave senior currency traders. Deutsche Bank was also cooperating with requests for information from regulators. Barclays, Citigroup, Deutsche Bank, HSBC, JPMorgan Chase, Lloyds, RBS, Standard Chartered, and UBS as of February 2014 had suspended, placed on leave, or fired 21 traders. Citigroup had also fired its

head of European spot forex trading.

BNP Paribas

BNP Paribas, France's biggest bank, announced in February 2014 that it had set aside US\$1.1bio for a possible fine for breaching US sanctions in countries including Iran, but also thought to include Sudan and Cuba. BNP said it had set aside the funds after talks with the US authorities, though it said there had been no discussion on the size of any potential penalty. "We've been doing a retrospective review for several years and we've basically now presented our findings to the US authorities," said BNP Chief Financial Officer, Lars Macheil. The US authorities involved are thought to include, the US Treasury Department's Office of Foreign Assets Control, the Manhattan District Attorney, the US Attorney for the Southern District of New York, the Justice Department, the Federal Reserve and the New York Department of Financial Services, which the person said are all involved in the probe, either declined comment or did not immediately respond to a request for comment.

Notes

Introduction

1. The Art of War by Sun Tzu – Special Edition. Translated and annotated by Lionel Giles (2005). El Paso Norte Press. ISBN 0-9760726-9-6. The Art of War is an ancient Chinese military treatise attributed to Sun Tzu (also referred to as "Sun Wu" and "Sunzi"), a high-ranking military general, strategist and tactician. It was believed to have been compiled during the period before the victory of the state of Qin in 221 BC, creating a unified China under the Qin Dynasty. The text is composed of 13 chapters, each of which is devoted to one aspect of warfare. It is commonly known to be the definitive work on military strategy and tactics of its time. It has been the most famous and important military treatise in Asia, for the last two thousand years. It has had an influence on Eastern and Western military thinking, business tactics, legal strategy and beyond.

Five Recommendations to “Effectively” combat Money Laundering

1. Whilst the term “money laundering” was invented and used for the first time only in the 20th Century, money laundering as a practice goes back much further. For details about the history of money laundering and the use of the term itself see “What is Money Laundering” at Page 14 onwards.

2. The United Nations Office on Drugs and Crime (UNODC) issued a report on 25 October 2011 entitled “Estimating illicit financial flows resulting from drug trafficking and other transnational organised crime,” which estimated that criminal proceeds, excluding tax evasion, would amount to some \$2.1 trillion or 3.6% of GDP in 2009, with US\$1.6 trillion being laundered. Of this total, the proceeds of transnational organised crime, such as drug trafficking, counterfeiting, human trafficking and small arms smuggling, would amount to 1.5% of 2009 global GDP, 70% of which or would likely have been laundered through the financial system. The Report stated that only 0.2% of illicit financial flows are currently being seized and frozen. UNODC [online]. 2011. Available from: <http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf> [Accessed 14 July 2013]. Note: A trillion is a number which has technically two definitions essentially the long scale definition traditionally used by the British and the short scale definition used by Americans. In Finance (the Bank of England has used the US definition for at least 20 years) and for the purposes of money laundering and as used by the UN and others in their work, the short scale definition is used so that a trillion is one million million or 1,000,000,000,000 As opposed to the long scale definition being one million million million or 1,000,000,000,000,000. Using the short scale definition a million is equal to a thousand thousands and a billion is equal to a thousand millions. In order to try to appreciate the size of a trillion consider the following: (i) How Long Ago Is a Trillion Seconds? - If you count backward, then: 1 million seconds = 12 days ago; 1 billion seconds = 31 years ago; 1 trillion seconds = 30,000 B.C. (approx); (ii) Height of a stack of US\$1000 bills?: If you stack a trillion-worth of \$1000 bills together, then: 1 million dollars = 4 inches high; 1 billion dollars = 364 feet high; 1 trillion dollars = 63 miles high (approx). Thankfully we are yet to hear about 1,000,000,000,000,000 or Quadrillion!

3. Havocscope [online]. 2013. Available from: <<http://www.havocscope.com/illicit-trade/>> [Accessed 14 July 2013]. According to Havocscope Illicit Trade is estimated at US\$1.79 trillion. The Havocscope Illicit Trade Value is the estimated value of the global black market. This figure is determined by combining the total value of 50 contraband products and illegal activities with the total value of black markets in 91 countries. The total values from both the products and countries are added together and divided by 2 in order to produce the Havocscope Illicit Trade Value. The Value of Products is estimated at US\$1.63 trillion and the Value of Countries at US\$1.94 trillion. Havocscope provides accurate, unbiased data by providing a centralized location for all information about the black market. All data listed within Havocscope's website is collected from credible public sources, such as newspapers, government reports and academic journals. Every single data point is listed with its original source. This allows users to see where the information has come from, judge the credibility of the source, and pursue further research if necessary. Havocscope maintains a strict policy of neutrality when dealing with issues surrounding the black market. They do not advocate for any position or offer any type of policy recommendations. They do not consult, advise, investigate or provide any ideas on how to change the black market. They are not funded by government agencies, foundations, or industry associations. Havocscope data has been used by the World Economic Forum in its 2011 Global Risks Report to highlight the issue of illicit trade. In 2012, the Council on Foreign Relations utilised Havocscope research when researching the issue of transnational crime for their Global Governance Monitor Project. Havocscope data has also been used in a wide range of publications such as Bloomberg News, National Geographic, The Atlantic

Monthly, and TheStreet.com.

4. Estimating the dimensions of the money flows related to corruption either in terms of how much is paid or how much is laundered as the profits of bribery is virtually impossible. Still the the World Bank has estimated between US \$1 trillion and US\$1.6 trillion dollars are lost globally each year to illegal activities. According to the World Bank, Corruption includes the abuse of public power for private gain, misappropriations of public goods, nepotism (favoring family members for jobs and contracts), and influencing the formulation of laws or regulations for private gain. World Bank [online]. 2013. available from <<http://web.worldbank.org/WBSITE/EXTERNAL/EXTABOU/TUS/0,contentMDK:23272490-pagePK:51123644-piPK:329829-theSitePK:29708,00.html>> [Accessed 14 July 2013].
5. The UK National Fraud Authority estimates that in 2010, Fraud cost the UK £38.4bio; see Fraud incl Tax Fraud and Cybercrime in Part 1 Section 1
6. According to the Association of Certified Fraud Examiners in the US Fraud costs US organisations more than US\$400 bio each year; see Fraud incl Tax Fraud and Cybercrime in Part 1 Section 1
7. See Note 2 above for details on the UNODC Report issued in October 2011. As far as transnational Organised crime is concerned the Report stated that their largest income still comes from illicit drugs, accounting for a fifth of all crime proceeds. For more details on organised crime and organised criminal gangs see Organised Crime in Part 1, Section 1 on Page 93 and Organised Criminal Gangs in Criminals and Terrorists in Part 2 Section 5.
8. Statement of Senator Carl Levin, Permanent Sub-Committee on Investigations Hearing on Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities, 9 November 1999. In fact Levin is quoting from one of the witnesses for the Sub-Committee, Raymond Baker, a guest scholar in Economic Studies at Brookings who estimates that US\$500bio to US\$1 trillion of international criminal proceeds are moved internationally and deposited into bank accounts annually. He estimates that half of this money comes to the US.
9. For more on the history that led to the signing of the Opium Convention see Drug Trafficking in Part 1 Section 1 and for brief details of the Convention itself see Money Laws and Regulation; AML Treaties, Conventions and Major Laws in Part 1 Section 3
10. For more on the history and developments of dangerous illegal drugs see Drug Trafficking in Part 1 Section 1
11. For more on the history and developments of organised crime and organised criminal gangs see Organised Crime in Part 1 Section 1 and Organised Criminal Gangs in Criminals and Terrorists in Part 2 Section 5.
12. For brief details on the Vienna Convention see Money Laundering Laws and Regulation; AML Treaties, Conventions and Major Laws in Part 1 Section 3.
13. According to FATF, money laundering is made up of the following 3 stages; placement, layering and integration. Placement - In the initial - or placement - stage of money laundering, the launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location; Layering - After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance; Integration - Having successfully processed his criminal profits through the first two phases the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.....FATF 2012, 40 Recommendations. This 3 stage process, the classic description of money laundering has also been described as “immersion”; generally inserting the proceeds of crime into the legitimate financial system, “heavy soaping” or disguising the trail of the monies as they pass through the financial system and finally the “spin dry” when the funds make it into legitimate income or assets. Furthermore FATF explain where Money Laundering may occur as follows: “As money laundering is a consequence of almost all profit generating crime, it can occur practically anywhere in the world. Generally, money launderers tend to seek out countries or sectors in which there is a low risk of detection due to weak or ineffective anti-money laundering programmes. Because the objective of money laundering is to get the illegal funds back to the individual who generated them, launderers usually prefer to move funds through stable financial systems. Money laundering activity may also be concentrated geo-graphically according to the stage the laundered funds have reached. At the placement stage, for example, the funds are usually processed relatively close to the under-lying activity; often, but not in every case, in the country where the funds

originate. With the layering phase, the launderer might choose an offshore financial centre, a large regional business centre, or a world banking centre – any location that provides an adequate financial or business infrastructure. At this stage, the laundered funds may also only transit bank accounts at various locations where this can be done without leaving traces of their source or ultimate destination. Finally, at the integration phase, launderers might choose to invest laundered funds in still other locations if they were generated in unstable economies or locations offering limited investment opportunities. "For Terrorism Finance, FATF, in their 2008 Terrorism Financing Typologies Report, also highlighted 3 stages, though these were not Placement, Layering and Integration, but Raising, Moving and Using funds, both criminally originated funds, where the 3 money laundering stages would still apply, but also to legally originated funds. As criminal activity, beyond drug trafficking become classified as predicate offences to Money Laundering, the original definitions and the classical 3 stages are unlikely to be sufficient to fully describe what money laundering is and how it is carried out, particular when considering, trade based laundering schemes, insider dealing and market manipulation, terrorism finance and tax evasion. Furthermore with advances in technology, electronic and mobile cash and digital currencies, we may need to consider whether money alone remains the principal concern. For more details see "What is Money Laundering," at Page 18.

14. Whilst the costs of compliance with applicable AML regulation are now both a cost of doing business and a necessary cost to protect a firm's reputation and from enforcement from those in the regulated sector, few estimates of the costs of compliance have been gathered. One study albeit somewhat dated now and as such likely to be a significant understatement, as AML regulations, expectations and enforcement risks for regulated firms have since this study significantly increased. Still for the period 2004/2005 the Corporation of London and the Institute of Chartered Accountants in England & Wales commissioned Z/Yen to investigate AML Costs of Compliance. The study assessed the perceived costs of UK Anti-Money Laundering Requirements compared with other jurisdictions including the USA, Germany, France and Italy. It was carried out between September 2004 and March 2005 and involved 34 personal interviews and an online survey that received 386 responses. From the report (published in June 2005), edited by Professor Michael Mainelli, Executive Chairman, of the Z/Yen Group. Whilst the study made two important points: firstly, that it is difficult to support increased regulatory action without a cost/benefit analysis and, secondly, it is difficult to support increased regulatory action when there is little or no feed-back. The study also recommended measures which would aid effectiveness in particular focussing on closing co-operation gaps. Areas which, if improved, could yield significant results in terms of practicality and effectiveness include: (i) joined up intelligence – insufficient resources are focussed on this and/or little or not enough time and effort is undertaken to ensure there is a collective pooling of intelligence about money laundering activity; (ii) feedback to financial services institutions regarding the quality and quantity of their reporting appears to be inadequate; and (iii) publicity of successful convictions and asset seizures should be given a far higher profile. The results of the study relating to the costs of AML compliance concluded that the costs for a number of leading jurisdictions was significant though those with major international financial centers and as such a greater number of regulated entities were the highest in absolute terms with the US and UK reported at a best estimate level of UK£253mio and the US at UK£1.2bio with just more than 0.02% of respective then GDP and Germany (UK£150 mio); France (UK£85mio); and Italy (UK£70 mio) with just below 0.02% of global GDP. The Study also reported that a third to a half of all costs were being borne by the Banking sector. According to Australian Institute of Criminology - http://www.aic.gov.au/media_library/aic/research/staff/aic-iiaa_smith_slides.pdf, Australian figures for 2004/2005 would have been UK£80 mio. Applying a 0.02% average to 2005 Global GDP (US\$45 trillion) would result in total costs of US\$9bio for the regulated sector. With top estimates in the 2004/05 Study averaging at approximately 20-25% above the best estimate and with every indication that today's expectations are significantly ahead of best estimates for 2004/05 a realistic minimum sum today should amount to at least 0.025% of 2012 GDP, (US\$71.6 trillion - <http://databank.worldbank.org/data/download/GDP.pdf>) or US\$17.9bio. According to a study by Reuter and Truman, published in their book Chasing Dirty Money, The Fight against Money Laundering; Institute of International Economics 200; ISBN: 0881323705; they estimated that "the total financial cost of the current system in the US is about US\$7bio annually, including costs borne by the government, financial and non-financial private sector institutions, and the general public."

15. Whilst the number of Suspicious transaction reports has increased year on year, we are beginning to see a plateauing off in many countries where Money Laundering Prevention programs can be seen as mature. Whilst the total global numbers are approaching 2 million per year, the largest contributor is the US, which in 2011 recorded 1,505,823 and even topped this in 2012 with 1,582,875. In order to compare numbers, the Australian Institute of Criminology looked at a number of countries to compare not only SAR's filed but also conviction rates using country available information. The Report focussed on annual data from either or during 2008/2009 or 2007 if none more recent and was entitled, "Extent of compliance and enforcement activity." (insert note) http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp113/07_extent.html. The results of this study showed that SAR's filed were as follows: Australia - 32,449 -2008/9; USA - 1,290,590 - 2008; UK - 228,834 - 2008/09; Belgium - 15,554 -2008; France - 14,565 -2008; Germany - 7,349 -2008; Singapore - 12,158 - 2008; Hong Kong - 15,838 -2007; Taiwan - 1,741 -2007

16. For more details about fines and penalties incurred by Financial Institutions see Part 2 Section 8 Enforcement Cases.

17. See Note 2 above

18. The US has aggressively expanded forfeiture powers as part of a broader growth to combat serious and Organised crime. Now there are more than 400 federal statutes allowing for forfeiture ranging from racketeering and drug-dealing to violations of the Northern Pacific Halibut Act, according to a December 2009 Congressional Research Service report. The report shows that seizure powers were extended to about 200 of those laws in 2000 in a major congressional overhaul of the forfeiture system. There has also been a shift with greater use of civil-forfeiture proceedings, in which assets can be taken without criminal charges being filed against the owner. In a civil forfeiture, the asset itself, not the owner of the asset, is technically the defendant. In such a case, the government must usually show by a preponderance of evidence that the property was connected to illegal activity. In a criminal forfeiture case, the government must first win a conviction against an individual, where the burden of proof is higher. Both Justice and Treasury Departments operate separate asset forfeiture programmes that are designed to prevent and reduce crime through the seizure and forfeiture of assets that represent the proceeds of or were used to facilitate crime. Annually the amounts seized by Justice and Treasury are increasing. For The Justice Fund, assets have been seized by numerous agencies including ATF, DEA, FBI and US marshals. For the Treasury Fund, assets have been seized by agencies such as the IRS, ICE, US Customs, Coast Guard and US Secret Service. On the 25th anniversary of the US DoJ asset forfeiture programme in 2009 Eric Holder US Attorney General said looking back over the development of the programme that "we see a forfeiture regime that has been transformed from centuries old laws designed to fight pirates enforce customs laws and fight illegal contraband into an array of modern law enforcement tools designed to combat 21st century criminals both at home and abroad." Holder also noted that since 2004 the DoJ has deprived criminals of over US\$13 bio net by its asset forfeiture activities. According to a 1992 Cato Institute study, The Justice Department's forfeiture fund held just US\$27 million in 1985. According to the GAO 12-736 Report "Justice Assets Forfeiture Fund" published in July 2012' in the 9 year period from fiscal years 2003 to 2011 AFF revenues totalled US\$11bio growing from US\$500mio in 2003 FY to US\$1.8bio in FY 2011, with 2004, US\$571mio; 2005, US\$612mio; 2006, US\$1.2bio; 2007, US\$1.66bio; 2008, US\$1.42bio; 2009, US\$1.45bio; and 2010, US\$1.79bio. Since 2006, an increase in the prosecution of fraud and financial crime cases led to substantial increases in AFF revenue. As a result of the increase in forfeitures resulting from money laundering and financial crime investigations in 2006 revenues doubled from the previous year from US\$612mio to US\$1,207 bio for the first time in AFF history breaking the US\$1bio level and since then continuing to grow to US\$1.8bio in 2011. According to DoJ's own Office of Inspector General (OIG) in an audit released in 2012 entitled, "Drug Enforcement Administration (DEA) adoptive seizure process and equitable sharing requests," the OIG report notes "for the period of October 1, 2000, through September 30, 2011, the DEA and other federal agencies processed over 150,644 seized assets valued at about US\$9.2bio of which US\$5.5bio (60%) originated from seizures processed by the DEA and US\$3.7bio (40%) originated from seizures processed by other federal agencies." The Audit also reported that forfeitures by assets in 2011 were the result of Administrative actions (48%), Civil (29%) and Criminal (23%). From 2003 to 2011 expenditures totalled 8.3 bio, with 2003 expenditures at 458 mio increasing to 1.3 bio in 2011. Expenditures are made up of 3 main areas - first payments to third parties or victims, second equitable sharing with police and other bodies involved and programme expenses. In 2011 US\$1.8bio was recovered whilst expenditures totalled 1.3 bio with 376 mio paid to third parties, 445 mio equitably shared and 491 mio the cost of the programme. The balance is carried over into the fund to cover future anticipated expenditure. Once used mainly as a tool against organised crime, mobsters and drug dealers, forfeiture is now much more broadly employed. For example recent figures released from the US Attorney's Office for the Southern District of New York, which covers Manhattan, covering actions and asset forfeitures for 2012, showed that this one office had its most successful year ever, reporting a haul of US\$2.98 billion in forfeitures and in addition US\$526.7 million from civil actions and US\$76.8 million in restitution, fines, and special assessments. To illustrate the change in those targeted the largest big ticket forfeitures related to the Madoff Ponzi Scheme, where collections of approximately \$2.22 billion have been made in 2012 from in particular the estate of one major investor beneficiary; from Science Applications International Corporation (SAIC), the primary contractor on New York City's "CityTime" payroll project, which forfeited \$500,392,977 in connection with its role in a fraud and kickback scheme, under a Deferred Prosecution Agreement; from John Rigas, the founder and former Chairman and Chief Executive Officer of Adelphia, and

Timothy Rigas, the former Chief Financial Officer, who were convicted for their participation in a massive securities fraud at Adelphia Communications Corp and who agreed to forfeit more than US\$728.9 million; from the internet gambling firm PokerStars who agreed to a first installment of US\$158.5 million from a US\$547mio settlement. Beyond these a number of financial institutions were subjected to forfeitures as a result of settlements, including Deutsche Bank & MortgageIT Fraud who forfeited US\$202.3 million; CitiMortgage, Inc who forfeited US\$158.3 million. Even the City of New York itself contributed US\$70 million for Medicaid irregularities. Again according to the release from the US Attorney's Office for the Southern District of New York Jan 2nd 2013, US\$4.389 billion was collected in asset forfeiture actions in FY 2012, which made the Southern District of New York the most successful responsible for 68% of the total. The U.S. Attorney's Office for the Southern District of New York also reported in the same release that, "Nationwide, the U.S. Attorneys' offices collected \$13.1 billion in criminal and civil actions during FY 2012, more than doubling the \$6.5 billion collected in FY 2011.

19. Whilst reliable consistent statistics are hard to come by, particularly as countries have failed to prioritize data capture and the organisation of data regarding successful asset recovery, there is nevertheless some available data which provides a useful commentary on the levels at which Countries strongly committed to the fight against money laundering and to the seizure and confiscation of criminal assets, have reached and indeed on their attitude to the collection and reporting of these results. The following statistics and related commentary relate primarily to figures obtained for the EU, with a focus on the UK and for Australia/New Zealand and the US. The reader should be aware that terms can mean different things in different countries, however in this commentary the terms asset seizure, confiscation and disposal are used to denote 3 distinct phases in the asset forfeiture process with seizure, usually the first where assets are only blocked, confiscation where ownership is transferred to the State or an instrument of the State and disposal where the asset is converted to cash after being sold and the final value of the asset is realized. Furthermore it should be understood that not all data is by any means comprehensive or up to date. In the case of Australia, according to statistics from the Australian Institute of Criminology (source: http://www.aic.gov.au/media_library/aic/research/staff/aic-iiia_smith_slides.pdf) Australia confiscated A\$49 mio in the Financial year 2006/07, this being a steady increase over the previous 2 years of A\$38 mio (2005/06) and A\$28 mio (2004/05). For New Zealand, since the Criminal Proceeds (Recovery) Act took effect in December 2009, about NZ\$29million worth of assets have been confiscated with a further NZ\$130.9million worth of assets seized or frozen. (insert source). In the case of the UK, figures are available for assets "recovered" (i.e. confiscated) in England, Wales and Northern Ireland (so excluding Scotland), (Source: <http://www.europarl.europa.eu/document/activities/cont/201206/20120627ATT47783/20120627ATT47783EN.pdf>) and these figures report that in 2003/04 £54.5mio was recovered, followed by steady increases in each of the years ahead as follows: 2004/05 - £84.4 mio; 2005/06 - £96mio; 2006/07 - £125.3mio and in 2007/08 - £135.7mio. More recently, the UK Government announced that the confiscation of criminal assets had reached £161m in the year to April 2011 with a further £800mio seized or frozen and another £50m returned to victims, still significantly short of its announced target of £1bn of assets confiscated a year. In part, to try to close the gap the UK government has launched a new strategy to introduce a new National Crime Agency to replace the current Serious Organised Crime Agency, to focus on Organised crime and the proceeds of crime from Organised crime which according to James Brokenshire, UK minister for crime and security is a strategy which, "provides a comprehensive national response across government, law enforcement, security and intelligence agencies...paving the way for the National Crime Agency, galvanising all those with a role to play in tackling organised crime. We need to address the threat at a local, national and international level in order to make a lasting impact." For the EU which of course includes the UK figures are available for some countries for asset seizures only, for confiscation only and for disposal only and some for combinations. The following are the results according to a Study by Matrix commissioned by the EU itself reporting in 2009 in a paper called the Final Asset Recovery Report, (Source: http://ec.europa.eu/home-affairs/news/intro/docs/20120312/final_asset_recovery_report_june_2009.pdf) which in addition to reporting on asset seizures, confiscations and disposals provided a detailed commentary on the ills afflicting the EU asset forfeiture system and provided detailed recommendations to improve effectiveness. The figures contained in the report identified that for the year 2007 or the year with most recent data prior to 2007 Countries had either seized, confiscated or disposed of criminal assets as follows: The UK had confiscated €157mio and disposed of €100mio; Spain had confiscated €83mio; The Netherlands seized €80mio and confiscated US\$22.6mio; Italy seized US\$656mio and confiscated US\$147mio; Belgium seized US\$52mio and confiscated € 48 mio; Germany seized \$218 mio; France seized 55.5 mio; Ireland seized €62.6 mio and disposed of €3.2mio; Poland seized €122mio; Finland seized € 23.6mio and confiscated €1.8mio; Lithuania seized €11.9mio; Austria confiscated €44mio; Sweden confiscated €1.8mio; Portugal confiscated € 2.4mio and the Czech Republic disposed of €23.6mio. According to a Report from the European Court of Auditors in 2009, (Source: insert link eu inside etc) seized assets amounted to €281mio in Germany, €185mio in France, £154mio pounds in Britain, €

50mio in the Netherlands. <http://www.euinside.eu/en/news/the-eu-lets-hit-the-crime-where-it-hurts-most-in-the-pocket>

20. The largest single recorded seizure of assets was announced in 2013 in Italy, when an Italian court ordered the acquisition of US\$1.9bio in mafia assets to be seized from Sicily's so called "Lord of the wind" or Vito Nicastri, a businessman with links to the Cosa Nostra or the Sicilian Mafia. Nicastri, who earned his nickname through his interests in vast wind farms, invested money made from extortion, drug sales and other illegal activities for the Sicilian Mafia's most sought-after fugitive, Matteo Messina Denaro, who is believed to be the Cosa Nostra's overall boss. In 2010, it emerged that Cosa Nostra was attempting to take millions of euros from both the Italian government and the EU by taking the generous grants on offer for investment in wind power and environmentally-friendly business. General Antonio Girone, then head of the national anti-Mafia agency DIA, said Mr Nicastri had built up a huge alternative energy business at the behest of the organised crime syndicate. In addition to halting the wind farm business interests of Mr Nicastri, Italian prosecutors also seized 66 bank accounts, as well as real estate property and other businesses, in Lazio and Calabria, and the northern region of Lombardy. Italy is ranked third in Europe, after Germany and Spain, for wind power, with almost 300 farms as of the end of 2009, according to Gestore Servizi Energetici, a public company that manages incentive programmes for renewable energy. Over the past decade, thanks to generous subsidies, wind farms have proliferated and increased in number substantially, with most, around 98% in the South of Italy.

21. A report entitled: The Globalization of Crime: A Transnational Organised Crime Threat Assessment, by the UNODC in June 2010 Available at: <<http://www.unodc.org/unodc/en/frontpage/2010/June/international-criminal-markets-have-become-major-centres-of-power-unodc-report-shows.html>> [Accessed 18 August 2013]; released at the Council of Foreign Relations in New York, looked at major trafficking flows of drugs (cocaine and heroin), firearms, counterfeit products, stolen natural resources and people (for sex and forced labour), as well as smuggled migrants. It also covers maritime piracy and cybercrime and shows how organised crime has globalized and turned into one of the world's foremost economic and armed powers. "Since crime creates instability, peace is the best way of containing crime," he said. "Criminals are motivated by profit: so let us go after their money," said UNODC Executive Director Antonio Maria Costa, adding that "We must increase the risks and lower the incentives that enable the bloody hand of organised crime to manipulate the invisible hand of competition". He called for more robust implementation of the UN Convention against Corruption, more effective anti-money laundering measures, and a crackdown on bank secrecy. He also stated that, "Today, the criminal market spans the planet: illicit goods are sourced from one continent, trafficked across another and marketed in a third." "Transnational crime has become a threat to peace and development, even to the sovereignty of nations," warned the head of UNODC. "Criminals use weapons and violence, but also money and bribes to buy elections, politicians and power - even the military," said Mr. Costa. "Despite the intrinsic difficulty of doing research on crime, UNODC was able to document the enormous power and global reach of international mafias," said Mr. Costa. The report makes a number of suggestions on how to deal with the threats posed by the globalization of crime, including "disrupting the market forces" behind these illicit trades and global responses on the basis of the UN Convention against Transnational Organised Crime (also known as the Palermo Convention), which was adopted in 2000. "Crime has internationalized faster than law enforcement and world governance," said Mr. Costa. "The Palermo Convention was created precisely to generate an international response to these transnational threats, but is often neglected," he said. "Governments that are serious about tackling the globalization of crime should spur the nations that are lagging behind in the implementation of the Convention," said the head of UNODC. "When States fail to deliver public services and security, criminals fill the vacuum," said Mr. Costa. "Reaching the Millennium Development Goals would be an effective antidote to crime, that in itself is an obstacle to development," he added. He also called for greater attention to criminal justice in peacebuilding and peacekeeping operations.

22. For more details about the FATF 2012 revised recommendations see Money Laundering Laws and Regulation; FATF work in 2012 on Page 248.

23. For more details about the FATF 2013 work on "effectiveness" see Money Laundering Laws and Regulation; FATF work in 2013 on Page 247.

24. http://www.fincen.gov/news_room/speech/pdf/20130227.pdf

25. Matrix (2009) ; Assessing the effectiveness of EU Member States' practices in the identification, tracking, freezing and confiscation of criminal assets. (online) [2009] Available at: <http://ec.europa.eu/home-affairs/news/intro/docs/20120313/final_asset_recovery_report_june_2009.pdf> [Accessed 13 April 2013]. Matrix was commissioned by the European Commission (EC) to: review current investigative, judicial and disposal phases of criminal asset recovery in EU Member States and identify good practice and obstacles to the effective implementation of asset recovery measures. Findings published in 2009 and recommendations were numerous, including insufficient resources

to cover expanding responsibilities, scepticism over the value of Asset recovery, challenges over cross border co-operation leads to inaction in many cases, conflicts with human rights and privacy laws, insufficient capacity to deal with non-cash assets, insufficient incentives, training and education and a lack of reporting and oversight to drive effectiveness and efficiency. Seven specific Recommendations were made to address the weaknesses and challenges faced and presented to the EC to consider and to act. These 7 Recommendations were: 1. A more realistic and motivational mission statement for the criminal asset recovery system should be produced, accompanied by a logic model which shows how all levels in the system contribute to the success of the mission. Assessing the effectiveness of EU Member States' practices in the identification, tracing, freezing and confiscation of criminal assets; 2. The EC should propose a system of incentives for improving the efficiency and effectiveness of criminal asset recovery. The incentive system will necessitate the keeping of adequate local operational records and the publishing of analyses including the auditing of system costs; 3. An expert task force should be provided to Member States to assist in the development of appropriate statistical systems; 4. Jurisdictions should be grouped into 'sets (families)' of similar Members to encourage local transfer of information and to simplify consultation; 5. A process review of EU institutions that support criminal asset recovery should be undertaken to ensure alignment with operational needs; 6. The practical EU initiatives already proposed which are widely supported should be implemented once our priority recommendations have been addressed but not before; 7. Appropriate training courses should be developed with the help of expert practitioners in Member States; training should be offered as part of an incentive package.

26. Available at: <<http://www.fatf-gafi.org/documents/guidance/bestpracticesonconfiscationrecommendations4and38andaframeworkforongoingworkonassetrecovery.html>> [Accessed on 18th August, 2013]

27. See also in Part 1 Section 3 Laws and Regulations - Copy the reference Note 75 - laws and regulations Part 1 Section 3

28. Non-bank FI's - In particular Money Services Businesses (MSB's). A 2005 US DEA study determined that MSB's both in the US and in Mexico, so called Casas de Cambio and Centros Cambiaro presented clear money laundering risks principally related to laundering the proceeds connected with the North American drug trade. In 2006 US FIU, FINCEN advised all US financial institutions formally about this threat. Notwithstanding, MSB's continue to feature in major money laundering cases.

29. Non-Financial Intermediaries representing real risks have been identified or referred to by numerous bodies; though many are either lightly or partly regulated or not regulated for money laundering purposes at all. FATF have identified a group they call, Designated Non Financial Professions and Businesses (DNFPB's) being professions and businesses that are seen as being attractive to money launderers and these are: Casino's, (when their customers engage in financial transactions above US\$3,000), Lawyers, Accountants and Trust and Company Service Providers, Dealers in Precious Metals and Stones (when their customers engage in CASH transactions above US\$15,000) and Real Estate Agents. Beyond DNFBP's, FATF have also identified Charities and Not for profit organisations where the risk of terrorist financing is potentially higher. Despite Politically Exposed Persons (PEP) being identified where the risk of bribery and corruption is potentially higher, this group is not subject to any direct oversight or regulatory scrutiny beyond those applied by the bank that maintains banking facilities with any PEP.

30. Havocscope [online]. 2013 Available from <http://www.havocscope.com/illicit_trade/> [Accessed 14 July 2013].

What is Money Laundering

1. Hegastratos, a Greek merchant, in 260 B.C. obtained an advanced loan from a shipment of corn through an agreement that allowed the lender to keep the ship and the shipment if payment was not received. Hegastratos attempted to keep the corn and sink the ship, leaving the lender without payment of goods. Hegastratos was caught in his fraud and died trying to escape.

2. Robinson, Jeffrey "The Laundrymen: Money Laundering the World's Third Largest Business": Arcade Publishing ISBN 978-1-55970-330-7 [1995].

3. Bernstein, C., Woodward, B. 2007. All The President's Men. Simon and Schuster.

4. Bernstein, C., Woodward, B. 1972. 'Bug Suspect got Campaign Funds', August 1 1972. Washington Post Online. [online] Available at: <<http://www.washingtonpost.com/wp-srv/national/longterm/watergate/articles/080172-1.htm>> [Accessed 14 July 2013]

5. International Money Laundering Information Bureau. 2013. History of Money Laundering. [online] Available at: <http://www.imlib.org/page1_hist.html> [Accessed 14 July 2013]

6. Federal Financial Institutions Examination Council (FFIEC). 1986. 'Money Laundering Control Act of 1986' [online] Available at: <http://www.ffcic.gov/bsa_aml_infobase/documents/regulations/ML_Control_1986.pdf> [Accessed 14 July 2013]

7. UN Office on Drugs and Crime. 1988. 'United Nations Convention Against Illicit Traffic in Narcotic Drugs

And Psychotropic Substances, 1988' [online] Available at: <http://www.unodc.org/pdf/convention_1988_en.pdf> [Accessed 14 July 2013]

8. UN General Assembly. 1999. 'International Convention for the Suppression of the Financing of Terrorism' [online] Available at: <<http://www.un.org/law/cod/finterr.htm>> [Accessed 14 July 2013]

9. Financial Action Task Force (FATF). 2012. 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations ('40 Recommendations')' [online] Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> [Accessed 14 July 2013]

10. European Union. 1991. Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering. [online] Available at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0308:EN:HTML>> [Accessed 14 July 2013]

11. The Crown Prosecution Service. 2010. 'Proceeds of Crime Act 2002 Part 7 – Money Laundering Offences'. [online] Available at: <http://www.cps.gov.uk/legal/p_to_r/proceeds_of_crime_money_laundering/> [Accessed 14 July 2013]

12. Gilmore, W. C. 1999. Dirty Money: The Evolution of Money Laundering Counter-measures. Council of Europe.

13. Financial Crimes Enforcement Network. 2013. 'History of Anti-Money Laundering Laws' [online] Available at: <http://www.fincen.gov/news_room/aml_history.html> [Accessed 14 July 2013]

14. UBS Global Anti Money Laundering Policy, since 2004

15. European Union. 2005. 'Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing'. Official Journal of the European Union. [online] Available at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:en:PDF>> [Accessed 14 July 2013]

16. European Union. 2012. [Press release] 'European Commission report on the application of the Third Anti-Money Laundering Directive - Frequently asked questions' 11/04/2012. [online] Available at: <http://europa.eu/rapid/press-release_MEMO-12-246_en.htm> [Accessed 14 July 2013]

17. MoneyGram. 2013. 'Anti-Money Laundering Compliance' [online] Available at: <<http://www.moneygram.com/MGICorp/Legal/MoneyLaundering/>> [Accessed 14 July 2013]

18. Swiss Bankers Association. 2013. 'The Fight Against Money Laundering' [online] Available at: <<http://www.swissbanking.org/en/home/dossiers-link/geldwaeschereibekämpfung.htm>> [Accessed 14 July 2013]

19. BusinessDictionary.com. 2013. 'Money Laundering' [online] Available at: <<http://www.businessdictionary.com/definition/money-laundering.html>> [Accessed 14 July 2013]

20. Interpol. 2013. 'Money Laundering' [online] Available at: <<http://www.interpol.int/Crime-areas/Financial-crime/Money-laundering>> [Accessed 14 July 2013]

21. Nasdaq. 2013. 'Money Laundering' [online] Available at: <<http://www.nasdaq.com/investing/glossary/m/money-laundering>> [Accessed 14 July 2013]

22. Financial Industry Regulatory Authority (FINRA). 2004. 'Small Firm Template: Anti-Money Laundering (AML) Programme: Compliance and Supervisory Procedures' [online] Available at: <<http://www.finra.org/Industry/Education/Materials/P038066>> [Accessed 14 July 2013]

23. The Organisation for Economic Co-operation and Development (OECD). 2002. 'Glossary of Statistical Terms: Money Laundering' [online] Available at: <<http://stats.oecd.org/glossary/detail.asp?ID=5081>> [Accessed 14 July 2013]

24. AUSTRAC: E-Learning. 2011. 'Introduction to Money Laundering' [online] Available at: <http://www.austrac.gov.au/elearning/mod1/mod_1_money_laundering_3.html> [Accessed 14 July 2013]

25. World Bank. 2003. Chapter 1: Money Laundering and Terrorist Financing: Definitions and Explanations [pdf] [online] Available at: <<http://www1.worldbank.org/finance/assets/images/01-chap01-f.qxd.pdf>> [Accessed 14 July 2013]

26. fides "terrorist financing refers to the processing of funds to sponsor of facilitate terrorist activity" etc pg 17

27. Isle of Man Financial Supervision Commission. 2013. 'Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT")' [online] Available at: <<http://www.gov.im/fsc/AML/?menuid=22866>> [Accessed 14 July 2013]

28. International Monetary Fund (IMF). 2013. 'Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT)' [online] Available at: <<http://www.imf.org/external/np/leg/amlcf/eng/aml1.htm>> [Accessed 14 July 2013]

29. Investopedia. 2013. 'Money Laundering Definition' [online] Available at: <<http://www.investopedia.com/>>

terms/m/moneylaundering.asp> [Accessed 14 July 2013]

30. FATF available at: <<http://www.fatf.com>> [Accessed 14 July 2003]

31. FATF available at: <<http://www.fatf.com>> [Accessed 14 July 2003]

32. The UN Office on Drugs and Crime (UNODC) issued a report on 25 October 2011 entitled "Estimating illicit financial flows resulting from drug trafficking and other transnational organised crime," which estimated that criminal proceeds, excluding tax evasion, would amount to some \$2.1 trillion or 3.6% of GDP in 2009, with US\$1.6 trillion being laundered. Of this total, the proceeds of transnational organised crime, such as drug trafficking, counterfeiting, human trafficking and small arms smuggling, would amount to 1.5% of 2009 global GDP, 70% of which could have been laundered through the financial system. The Report stated that only 0.2% of illicit financial flows are currently being seized and frozen. UNODC [online]. 2011. Available from: <http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf> [Accessed 14 July 2013].

Note: A trillion is a number which has technically two definitions essentially the long scale definition traditionally used by the British and the short scale definition used by Americans. In Finance (the Bank of England has used the US definition for at least 20 years) and for the purposes of money laundering and as used by the UN and others in their work, the short scale definition is used so that a trillion is one million million or 1,000,000,000,000 As opposed to the long scale definition being one million million million or 1,000,000,000,000,000,000. Using the short scale definition a million is equal to a thousand thousands and a billion is equal to a thousand millions. In order to try to appreciate the size of a trillion consider the following: (i) How Long Ago Is A Trillion Seconds? - If you count backward, then: 1 million seconds = 12 days ago; 1 billion seconds = 31 years ago; 1 trillion seconds = 30,000 B.C. (approx); (ii) Height of a stack of US\$1000 bills?: If you stack a trillion-worth of \$1000 bills together, then: 1 million dollars = 4 inches high; 1 billion dollars = 364 feet high; 1 trillion dollars = 63 miles high (approx). Thankfully we are yet to hear about 1,000,000,000,000,000 or Quadrillions!

33. Estimating the dimensions of the money flows related to corruption either in terms of how much is paid or how much is laundered as the profits of bribery is virtually impossible. Still the World Bank has estimated between US \$1 trillion and US\$1.6 trillion dollars are lost globally each year to illegal activities. According to the World Bank, Corruption includes the abuse of public power for private gain, misappropriations of public goods, nepotism (favoring family members for jobs and contracts), and influencing the formulation of laws or regulations for private gain. World Bank [online]. 2013. available from <<http://web.worldbank.org/WBSITE/EXTERNAL/EXTABOUTUS/0,,contentMDK:23272490-pagePK:51123644-piPK:329829-theSitePK:29708,00.html>> [Accessed 14 July 2013].

34. The figure of US\$2.75 trillion is an estimate arrived at by applying available estimates for the UK (see note 5, Five Recommendations to effectively combat money laundering) and for the US see note 6, 5 Recommendations to effectively combat money laundering to other countries using global GDP figures. See also Part 1, Section 1, Fraud incl Tax Fraud and Cybercrime.

35. The figure of US\$4.5 trillion is an estimate based on applying estimates and applying them to global GDP figures. See Part 1, Section 1, Fraud incl Tax Fraud and Cybercrime for more details.

Part 1 - Section 1 Money Laundering Crimes

Introduction

1. Financial Action Task Force, 2012. Financial Action Task Force. The FATF Recommendations, [Online]. Available at: <http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> [Accessed 5 May 2013].

2. Estimating the dimensions of the money flows related to corruption either in terms of how much is paid or how much is laundered as the profits of bribery is virtually impossible. Still the World Bank has estimated between US \$1 trillion and US\$1.6 trillion dollars are lost globally each year to illegal activities. According to the World Bank, Corruption includes the abuse of public power for private gain, misappropriations of public goods, nepotism (favoring family members for jobs and contracts), and influencing the formulation of laws or regulations for private gain. World Bank [online]. 2013. available from <<http://web.worldbank.org/WBSITE/EXTERNAL/EXTABOUTUS/0,,contentMDK:23272490-pagePK:51123644-piPK:329829-theSitePK:29708,00.html>> [Accessed 14 July 2013].

3. Havoscope - The Black Market Economy. 2013. Havoscope: Global Black Market Information. [ONLINE]. Available at: <<http://www.havoscope.com>>. [Accessed 5 May 13].

Bribery & Corruption

1. Ribadu, N. (2006 September). Address to the World Bank and International Monetary Fund Annual Meetings

presented in Singapore.

2. World Bank [online]. (2004). Available from: <<http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:20190295-menuPK:34457-pagePK:34370-piPK:34424-theSitePK:4607,00.html>>, [Accessed 5 May 2013].

3. UN News Centre [online]. (2009). Available from: <<http://www.un.org/apps/news/story.asp?NewsID=40189#UYa6HcqwWSO>>. [Accessed 5 May 2013].

4. The World Bank [online]. (2010). Available from: <<http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:22609142-pagePK:64257043-piPK:437376-theSitePK:4607,00.html>>. [Accessed 5 May 2013].

5. Transparency International [online]. (2014). Available from: <<http://www.bpi.transparency.org/bpi2011/results/>>. [Accessed 8 April 2014].

6. Transparency International [online]. (2014). Available from: <<http://www.transparency.org/cpi2013>>. [Accessed 8 April 2014].

7. Russian Oligarchs emerged in the post Soviet collapse, where a number of individual businessmen quickly acquired huge wealth during the privatization in Russia in the 1990s. The original Oligarchs were business entrepreneurs who started under Mikhail Gorbachev during his period of market liberalization or perestroika, which saw the start of private business and commerce develop. After Boris Yeltsin took office, the oligarchs emerged as well-connected entrepreneurs who exploited the governments lack and desperate need for finance and the weaknesses of the government designed voucher privatization schemes to acquire state assets at firesale prices. The most influential and well known oligarchs from the Yeltsin era were Boris Berezovsky, Mikhail Khodorkovsky, Alex Konanykhin, Mikhail Fridman, Vladimir Gusinsky, Vitaly Malkin and Vladimir Potanin. Potanin, Malkin and Fridman are the only ones to have made it to the Putin era as a number have lost their status, either banished, exiled or imprisoned. In particular, Vladimir Gusinsky (MediaMost) and Boris Berezovsky avoided direct legal proceedings by leaving Russia, whilst the most prominent, Mikhail Khodorkovsky (Yukos oil), was arrested in October 2003, and sentenced to 9 years, which was subsequently extended to 14 years imprisonment. Most observers believe this clash resulted from Khodorkovsky's increased interest in Politics. The arrest came 3 years after Putin met 21 of Russia's oligarchs informing them that their political power was at an end, that they would not be allowed to wield influence in the Kremlin and should stay out of political matters. They were offered the olive branch however of keeping the companies they won during Russia's privatisations. The most famous oligarchs that have risen during the Putin era include Roman Abramovich, Oleg Deripaska and Mikhail Prokhorov.

8. In 2010 the SEC's Enforcement Division created a specialised unit to further enhance its enforcement of the FCPA, bringing marquee names to account including the following: i) Innospec: The US-based chemical manufacturer pled guilty to paying bribes to Indonesian and Iraqi government officials to secure sales of a fuel additive, in 2010. The case was also prosecuted in Indonesia and the UK. Innospec paid US\$40.2mio in fines to the DOJ, SEC and UK Serious Fraud Office. ii) ABB: The Swiss-based global provider of power and automation products was charged and fined for using a US subsidiary to pay bribes to officials at Mexico's largest power company as well as to pay kickbacks to Iraq to obtain contracts under the UN Oil for Food Programme. ABB agreed to a US\$39.3mio settlement in 2010. iii) Alliance One/Universal Corp: Two tobacco companies were charged for making more than US\$5mio in secret payments to government officials in Thailand and around the world to illicitly obtain tobacco sales contracts. The companies paid US\$28.3mio to settle SEC and criminal charges in 2010. iv) DaimlerChrysler: The Germany-based automobile manufacturer was charged for its repeated and systematic practice of paying bribes to foreign government officials to secure business in Asia, Africa, Eastern Europe, and the Middle East. Daimler paid US\$185mio to settle SEC and criminal charges in 2010. v) General Electric: GE, and two subsidiaries, Ionics Inc, and Amersham plc were charged with making illegal kickback payments, in the form of cash, computer equipment, medical supplies, and services to the Iraqi government in order to obtain UN Oil for Food Programme contracts. GE paid US\$23mio to settle the charges in 2010. vi) ENI: The Italian energy giant and one of its subsidiaries in the Netherlands were charged with a decade-long bribery scheme that included deliveries of cash-filled briefcases and vehicles to Nigerian government officials to win construction contracts. Snamprogetti and ENI jointly paid US\$365mio to settle SEC and criminal charges in 2010. vii) Technip SA: The Paris-based global engineering company was charged for bribing Nigerian government officials over a 10-year period in order to win construction contracts worth more than US\$6bio. Technip agreed to pay US\$338mio to settle SEC and criminal charges in 2010. viii) Allianz SE: SEC charged the Germany-based insurer with violating the books and records and internal controls provisions of the FCPA for improper payments to government officials in Indonesia that resulted in US\$5.3mio in profits. Allianz agreed to pay more than US\$12.3mio to settle the SEC's charges. ix) Diageo: the UK-based premium alcohol and spirits producer made improper payments totaling approximately US\$2.7mio through its subsidiaries in India, Thailand and South Korea to obtain sales and tax breaks worth over US\$61mio.

The Company entered into a settlement with the SEC in 2010 accepting penalties totaling over US\$16mio. Additionally, the Korean authorities convicted five former Diageo Korea employees. x) Magyar Telekom: SEC charged the largest telecommunications provider in Hungary and three of its former top executives with bribing government and political party officials in Macedonia and Montenegro. The firm and its parent company agreed to pay US\$95mio to settle civil and criminal charges in 2011. xi) JGC: This Japanese company that is not a US issuer itself and committed no acts in the US, nevertheless was held accountable as a joint venture partner that paid bribes to Nigerian officials to secure development contracts for liquefied natural gas facilities, illustrating just how aggressively the US asserts its jurisdiction. US jurisdiction was obtained by virtue of its partnership with a US company and US issuers, and because the bribes were paid with US dollars, processed through US correspondent accounts. JGC entered into a two-year DPA with the US DOJ, agreeing to pay US\$218.8mio in fines in 2011. xii) Maxwell Technologies: The US-based electronic and power producer, entered into a three-year DPA with the DOJ, on charges that its Swiss subsidiary had paid US\$2.5mio on inflated invoices as "sales commissions" to a sales agent who passed it on to officials at Chinese state-owned entities to secure contracts. Maxwell Technologies knew of the bribes for six years before it took effective action to stop them. Ultimately, the company paid US\$8mio in criminal fines and US\$6.38mio in disgorgement of profits in 2011. xiii) Armor Holdings: The SEC charged the US-based body armor supplier for illicit payments to UN officials to obtain contracts related to U.N. peacekeeping missions. Armor Holdings agreed to an SEC settlement of US\$5.7mio and a criminal fine of US\$10.29mio in 2011. xiv) Tenaris: The SEC sanctioned in 2011 the global manufacturer of steel pipe products for bribing Uzbekistan government officials during a bidding process to supply pipelines for transporting oil and natural gas. Tenaris agreed to pay US\$5.4mio under a Deferred Prosecution Agreement, and paid a US\$3.9mio criminal fine. xv) Aon Corporation: US-based global insurer, via its UK subsidiary, charged with bribes, totaling \$3.6 million, including training, travel and entertainment, offered in Myanmar, Bangladesh, Indonesia, and Vietnam, and other countries to government officials who were responsible for awarding insurance contracts. The charges focussed on violations of the books and records and internal controls provisions of the FCPA. Aon entered into a two-year non-prosecution agreement (NPA) with DOJ in 2011 and agreed to pay a US\$1.76mio fine, and simultaneously settled with the SEC for US\$14,545,020 in disgorgement and pre-judgment interest. The UK Financial Services Authority (FSA) had imposed a fine of £5.25mio. xvi) Johnson & Johnson: The US-based provider of medical devices, pharmaceuticals, and consumer healthcare products, was charged for its alleged conduct in making improper payments to employees of state-owned healthcare providers in various countries to obtain contracts, including to doctors in several European Countries, to Iraq to illegally win business and elsewhere. J&J agreed to pay US\$70mio to settle cases brought by the SEC and DOJ and enter into a DPA in 2011. xvii) IBM: International Business Machines Corp was charged in 2011 with providing improper cash, gifts, overseas travel for training and entertainment in order to secure sales of its products to government officials in China and South Korea in order to secure the sale of IBM products. IBM agreed to pay US\$10mio to settle the SEC's charges. IBM agreed to pay penalties to the SEC amounting to US\$82mio in 2011. xviii) Tyson Foods: The US-based worldwide chicken manufacturer charged for making illicit payments to two Mexican government veterinarians responsible for certifying its Mexican subsidiary's chicken products for export sales. Tyson Foods agreed to pay US\$5mio in 2011 to settle charges. xix) Alcatel: The French Company paid bribes to employees of Telekom Malaysia, a 43% state-owned company, which led to FCPA charges, which indicates a broad definition of foreign officials. Besides bribes to government officials in Malaysia for information leading to a successful bid from Telekom Malaysia, there were also alleged bribes paid to Taiwanese legislators and a minister by consultants to obtain contracts with the Taiwan Railway Administration. Alcatel entered into a three-year deferred prosecution agreement (DPA) with DOJ in 2011 and the three charged subsidiaries pled guilty. Penalties totaling US\$135.5mio were incurred, with fines from DOJ amounting to US\$92mio, in addition to US\$45,372,000 in disgorgement of profits imposed by the SEC. The Company also in an earlier case in 2010 agreed to pay US\$137mio to settle charges for using consultants who performed little or no legitimate work to funnel bribes to government officials and win contracts in Latin America and Asia. xx) Eli Lilly & Company: SEC charged the US based pharmaceutical company for improper payments its subsidiaries made to foreign government officials to win business in Russia, Brazil, China, and Poland. Eli Lilly agreed to pay more than US\$29mio in 2012 to settle the charges. xxi) Tyco International: SEC charged the Swiss-based global manufacturer with violating the FCPA when subsidiaries arranged illicit payments to foreign officials in more than a dozen countries. Tyco agreed to pay US\$26mio in 2012 to settle the SEC's charges and resolve a criminal matter with the Justice Department. xxii) Pfizer: SEC charged the pharmaceutical company for illegal payments made by its subsidiaries to foreign officials in Bulgaria, China, Croatia, Czech Republic, Italy, Kazakhstan, Russia, and Serbia to obtain regulatory approvals, sales, and increased prescriptions for its products. Pfizer and recently acquired Wyeth LLC - charged with its own FCPA violations - agreed to pay in 2012 a combined US\$45mio in their settlements.

xxiii) Smith & Nephew: SEC charged the UK based medical device company with violating the FCPA when its US and German subsidiaries bribed public doctors in Greece for more than a decade to win business. The company and its US subsidiary agreed to pay more than US\$22mio in 2012 to settle civil and criminal cases. xxiv) In 2013, French oil giant Total S.A. agreed to pay US\$398mio in penalties and disgorgement for bribing an Iran official to gain access to oil and gas fields. Total will pay a criminal penalty to the DOJ of US\$245.2mio. It received a three-year deferred prosecution agreement that requires appointment of an independent compliance monitor. In its settlement with the SEC, Total will disgorge profits of US\$153mio. That's the second biggest disgorgement in FCPA history. It paid at least US\$60mio in bribes for access to the Iran oil and gas fields, and made more than US\$150 in profit, the enforcement agencies said. A criminal information filed in federal court in Virginia charged Total with one count of conspiracy to violate the FCPA's antibribery provisions, one count of violating the internal controls provisions, and one count of violating the books and records provisions. The SEC settled with Total through an administrative order and didn't file a complaint against Total in court. In 1995, the DOJ said, Total tried to obtain a concession from the National Iranian Oil Company to develop the Sirri A and E oil and gas fields. An Iranian official in the negotiations designated an intermediary to be a Total consultant. Total paid the consultant \$16 million in bribes under the phony consulting agreement over the next two and a half years. Total retained another consultant in 1997 designated by the same official and paid about US\$44mio under the agreement. In return, Total secured the rights to develop part of South Pars, the world's largest gas field. 'Total attempted to cover up the true nature of the illegal payments,' the SEC said, 'by entering into sham consulting agreements with intermediaries of the Iranian official and mischaracterizing the bribes in its books and records as legitimate "business development expenses" related to the consulting agreements.' Total also was charged today by the prosecutor of Paris (François Molins, Procureur de la République) of the Tribunal de Grande Instance de Paris for violations of French laws.

French oil giant Total S.A. agreed in 2013 to pay US\$398mio in penalties and disgorgement for bribing an Iran official to gain access to oil and gas fields. Total will pay a criminal penalty to the DOJ of US\$245.2mio. It received a three-year deferred prosecution agreement that requires appointment of an independent compliance monitor. In its settlement with the SEC, Total will disgorge profits of US\$153mio. That's the second biggest disgorgement in FCPA history. It paid at least US\$60mio in bribes for access to the Iran oil and gas fields, and made more than US\$150 in profit, the enforcement agencies said. In 1995, the DOJ said, Total tried to obtain a concession from the National Iranian Oil Company to develop the Sirri A and E oil and gas fields. An Iranian official in the negotiations designated an intermediary to be a Total consultant. Total paid the consultant US\$16mio in bribes under the phony consulting agreement over the next two and a half years. Total retained another consultant in 1997 designated by the same official and paid about US\$44mio under the agreement. In return, Total secured the rights to develop part of South Pars, the world's largest gas field. Total attempted to cover up the true nature of the illegal payments, the SEC said, 'by entering into sham consulting agreements with intermediaries of the Iranian official and mischaracterizing the bribes in its books and records as legitimate "business development expenses" related to the consulting agreements.' Total was also charged by the prosecutor of Paris (Procureur de la République) of the Tribunal de Grande Instance de Paris for violations of French laws.

Counterfeit & Piracy of Products

1. Colton, C. C. (1820). *Lacon Or Many Things In Few Words: Addressed To Those Who Think*. London: William Tegg. Available from: <<http://books.google.co.uk/books?id=gTECAAAQAAJ>>. [Accessed 6 May 2013].
2. OECD Organisation for Economic Co-operation and Develop, 2008. *The Economic Impact of Counterfeiting and Piracy*. Pap/Ado Edition. OECD Publishing.
3. OECD (2009). *Magnitude of Counterfeiting and Piracy of Tangible Products: An Update*. [online]. Available from: <<http://www.oecd.org/sti/ind/4408872.pdf>>. [Accessed 6 May 2013].
4. Havocscope - The Black Market Economy [online]. (2013). Available from: <<http://www.havocscope.com/category/counterfeiting/>>. [Accessed 6 May 2013].
5. International Chamber of Commerce: The World Business Organisation [online]. (2013). Available from: <<http://www.iccwbo.org/products-and-services/fighting-commercial-crime/counterfeiting-intelligence-bureau/>>. [Accessed 6 May 2013].
6. Ranking of Counterfeit Goods. 2013. *Ranking of Counterfeit Goods*. [online]. Available at: <<http://www.havocscope.com/counterfeit-goods-ranking/>>. [Accessed 6 May 2013].
7. Frontier Economics (2011). *Estimating the global economic and social impacts of counterfeiting and piracy*. Frontier Economics Ltd: London.
- 7b.Riano, J. & Hodess, R. (2008). *Bribe Payers Index*. Germany: Transparency International.

8. Department of Homeland Security: US Customs and Border Protection and US Immigration and Customs Enforcement (2005). FY 2005 Top IPR Commodities Seized. Available from: <http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/ipr_communications/seizure/trading/fy05_midyear_stats.ctt/fy05_ipr_midyear.pdf>. [Accessed 6 May 2013].
9. US Customs and Border Protection and US Immigration and Customs Enforcement (2009). Intellectual Property Rights Seizure Statistics: Fiscal Year 2009. Available from: <http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/ipr_communications/seizure/fy09_stats.ctt/fy09_stats.pdf>. [Accessed 6 May 2013].
10. Counterfeit - definition of Counterfeit by the Free Online Dictionary, Thesaurus and Encyclopedia. 2013. Counterfeit - definition of Counterfeit by the Free Online Dictionary, Thesaurus and Encyclopedia. [online] Available at: <<http://www.thefreedictionary.com/Counterfeit>>. [Accessed 06 May 2013].
11. Piracy - definition of piracy by the Free Online Dictionary, Thesaurus and Encyclopedia. 2013. piracy - definition of piracy by the Free Online Dictionary, Thesaurus and Encyclopedia. [online] Available at: <<http://www.thefreedictionary.com/piracy>>. [Accessed 06 May 2013].
12. The FATF Recommendations (2012). International Standards on Combating Money Laundering and the Financing of Terrorism. Paris: FATF.
13. Statute of Anne, London (1710), Primary Sources on Copyright (1450-1900), eds L. Bently & M. Kretschmer, <www.copyrighthistory.org>
14. Kochan, N. (2008). Counterfeiting - the \$650b challenge. Available from: <http://www.amlmagazine.com.au/amlwr/_assets/main/lib90004/counterfeiting%20the%20650b%20challenge_issue15_november08.pdf> [Accessed 6 May 2013].
15. Irish, J. (2010). Customs group to fight \$200 bln bogus drug industry. Available from: <<http://www.reuters.com/article/2010/06/10/us-customs-drugs-idUSTRE65961U20100610>>. [Accessed 6 May 2013].
16. Hirschler, B. (2012). Row flares over global fight against fake medicine. Available from: <<http://www.reuters.com/article/2012/11/14/us-pharmaceuticals-fake-who-idUSBRE8AC19V20121114>>. [Accessed 6 May 2013].
17. Roberts, M. (2012). Third of malaria drugs 'are fake'. Available from: <<http://www.bbc.co.uk/news/health-18147085>>. [Accessed 6 May 2013].
18. Weede, E. (2012). Liberia: How Are Counterfeit Medicines Brought Into the Country. Available: <<http://al-africa.com/stories/201205211220.html>>. [Accessed 6 May 2013].
19. English.news.cn [online]. (2011). Available from: <http://news.xinhuanet.com/english/china/2011-12/20/c_131317339.htm>. [Accessed 6 May 2013].
20. Mahgul Rind, H. (2012). IPR challenges drive foreign pharmaceuticals away from Pakistan. Available: <<http://www.thenews.com.pk/Todays-News-3-107722-IPR-challenges-drive-foreign-pharmaceuticals-away-from-Pakistan>>. [Accessed 6 May 2013].
21. Castellani, J. J. (2012). Counterfeit medicine threat knocking on America's doors. 28 March 2012. The Hill's Congress Blog: Where lawmakers come to blog [online]. [Accessed 6 May 2012]. Available from: <<http://thehill.com/blogs/congress-blog/homeland-security/218699-john-j-castellani-president-and-ceo-pharmaceutical-research-and-manufacturers-of-america>>.
22. IHS (2012). Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defense Industry and National Security. Press release, issued 14 February 2012.
23. O'Donnell, J.. (2012). Counterfeit products are a growing, and dangerous, problem. Available: <<http://usatoday30.usatoday.com/money/perfi/columnist/odonnell/story/2012-06-01/confident-consumer-jayne-odonnell/55406774/>>. [Accessed 6 May 2013].
24. InnovationNewsDaily Staff. (2012). US Missile Defense Seeks Fix for Counterfeits. Available: <<http://www.livescience.com/20236-missile-defense-fix-counterfeits.html>>. [Accessed 6 May 2013].
25. The Associated Press. (2011). Lawmakers: Counterfeit electronics flood Pentagon supply. Available: <http://usatoday30.usatoday.com/news/washington/story/2011-11-07/pentagon-counterfeit-electronics/51112630/1?csp=34n_ews>. [Accessed 6 May 2013].
26. Roberts, J.J. (2012). Gigaom [online]. Available from: <<http://gigaom.com/2012/05/24/google-takes-down-1-2-million-search-links-a-month-over-piracy-copyright-issues/>>. [Accessed 6 May 2013].
27. Google Transparency Report [online]. (2013). Available from: <<http://www.google.com/transparencyreport/removals/copyright/>>. [Accessed 6 May 2013].
28. Fletcher, O. & Dean, J.(2011). The Wall Street Journal [online]. Available from: <<http://online.wsj.com/article/SB10001424052702303654804576347190248544826.html>>. [Accessed 6 May 2013].
29. Business Software Alliance (2012). 2011 BSA Global Software Piracy Study: Ninth Edition. BSA Worldwide Headquarters: Washington.
30. Business Software Alliance (2011). 2010 Piracy Study. BSA Worldwide Headquarters: Washington.
31. Havocscope. (2011). Software Piracy Losses by Country. Available: <<http://www.havocscope.com/software-piracy-losses-by-country/>>. [Accessed 6 May 2013].
32. Interlandi, J. (2010). The Fake Food Detectives. Available: <<http://www.thedailybeast.com/news-week/2010/02/07/the-fake-food-detectives.html>>. [Accessed 6 May 2013].
33. Byrne, J. (2009). UK Food Safety Agency in Fraud Crackdown. Available: <<http://www.foodproductiondaily.com/a-Safety/UK-food-safety-agency-in-fraud-crackdown/>>. [Accessed 6 May 2013].
34. Warner,K., Timme, W., Lowell, B. & Hirshfield, M. (2011). Oceana Study Reveals Seafood Fraud Nationwide. Oceana [online]. Available from: <http://oceana.org/sites/default/files/National_Seafood_Fraud_Testing_Results_FINAL.pdf>. [Accessed 6 May 2013].
35. Bottemiller, H. (2013). "Honeygate" Sting Leads to Charges for Illegal Chinese Honey Importation. Available: <<http://www.foodsafetynews.com/tag/honey/>>. [Accessed 6 May 2013].
36. McDonald, J. (2009). Arrests in Fake Baby Formula Case. Available: <<http://www.cbsnews.com/2100-162-616432.html>>. [Accessed 6 May 2013].
37. Interpol (2011). Tonnes of illicit foods seized across Europe in INTERPOL-Europol led operation. Press release, issued 6 December 2011.
38. Bowman, Z (2011). Report: Counterfeit parts overwhelm China, include fake airbags, oil seals. 16 February 2011. Auto News [online]. [Accessed 6 May 2013]. Available from: <<http://www.autoblog.com/2011/02/16/report-counterfeit-parts-overwhelm-china-include-fake-airbags/>>.
39. George, J. (2011). 25% auto parts are counterfeit. Available: <<http://www.emirates247.com/business/economy-finance/25-auto-parts-are-counterfeit-2011-09-28-1.421095>>. [Accessed 6 May 2013].
40. AFP (2011). French agents in endless hunt for counterfeits. Available: <<http://www.independent.co.uk/life-style/french-agents-in-endless-hunt-for-counterfeits-2297201.html>>. [Accessed 6 May 2013].
41. Havocscope. (2013). Fakes in EU Replacement Auto Parts Industry. Available: <<http://www.havocscope.com/fakes-in-eu-replacement-auto-parts-industry>>. [Accessed 6 May 2013].
42. Economic Times [online]. (2011). Available from: <<http://economictimes.indiatimes.com/news/news-by-industry/auto/auto-components/counterfeit-auto-parts-costing-government-rs-2200-crore-per-annum/article-show/7547841.cms>>. [Accessed 6 May 2013].
43. Jakarta Post [online]. (2010). Available from: <<http://www.thejakartapost.com/news/2011/11/04/fake-products-cost-ri-ri-432t-lost-taxes.html>>. [Accessed 6 May 2013].
44. Toy Industries of Europe (2011). Counterfeit toys worth almost €25 billion seized at EU borders. Press release, issued 14 July 2011.
45. CPD (2011). IPR Seizures Statistics, FY 2010. Available: <http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/pubs/seizure/seizure_stats_fy2010.ctt/seizure_stats_fy2010.pdf>. [Accessed 6 May 2013].
46. Havocscope [online]. (2013). Available from: <<http://www.havocscope.com/?s/toy industries of europe>>. [Accessed 6 May 2013].
47. Havocscope [online]. (2013). Available from: <<http://www.havocscope.com/counterfeit-goods-ranking/>>. [Accessed 7 May 2013].
48. Hong, S. (2012). Half of all netizens here access illegal download sites. Available: <<http://news.asiaone.com/News/Latest%2BNews/Singapore/Story/A1Story20120503-343530.html>>. [Accessed 7 May 2013].
49. Long, V. (2012). Ignoring digital copyright, Vietnamese openly use stolen products. Available: <<http://english.vietnamnet.vn/en/science-technology/21024/ignoring-digital-copyright--vietnamese-openly-use-stolen-products.html>>. [Accessed 7 May 2013].
50. The American Assembly (2011). Copyright Infringement and Enforcement in the US. Columbia University: New York. Available at: <<http://piracy.americanassembly.org/wp-content/uploads/2011/11/AA-Research-Note-Infringement-and-Enforcement-November-2011.pdf>>. [Accessed 7 May 2013].
51. Hachman, M. (2011). Piracy Pays for Itself, Swiss Government Says. Available: <<http://www.pcmag.com/article/2/0,2817,2397173,00.asp>>. [Accessed 7 May 2013].
52. Roxborough, S. (2012). Study: Cost of German Music Piracy at \$660 Million. Available: <<http://www.hollywoodreporter.com/news/piracy-germany-336283>>. [Accessed 7 May 2013].
53. Chu, K. (2012). Hong Kong Film Piracy on YouTube Amounts to \$308 Million Loss. Available: <<http://www.hollywoodreporter.com/news/hong-kong-film-piracy-youtube-314976>>. [Accessed 7 May 2013].
54. Linao, G. (2012). Philippine film industry struggles to get out of slump. Available: <<http://ibikyamasr.com/58724/philippine-film-industry-struggles-to-get-out-of-slump/>>. [Accessed 7 May 2013].
55. Watkins, D. (2012). Asia's digital divide poses challenge for music industry. Available: <<http://www.google.com/>>.

- hostednews/afp/article/ALeqM5gFziRYJxYF-tOcg8degkAQqF50zQ?docId=CNG.8209df825c55769257f90f0595d
a4a66.1c1>. [Accessed 7 May 2013].
56. Collett-White, M. (2012). Music sales fall again in 2011, but optimism grows. Available: <<http://www.reuters.com/article/2012/01/23/music-idUSL6E8CL0A720120123>>. [Accessed 7 May 2013].
57. Havocscope [online]. (2013). Available from: <<http://www.havocscope.com/countries/ranking/>>. [Accessed 7 May 2013].
58. Sporting Goods Manufacturers Association [online]. (2011). Available from: <<http://www.sgia.org/publicpolicy/intellectualpropertyactiveissues/counterfeitsseizuresup>>. [Accessed 7 May 2013].
59. Stone, H. (2012). Colombia Sees Flood of Pirated Chinese Shoes. Available: <<http://insightcrime.org/insight-latest-news/item/2502-colombia-sees-flood-of-pirated-chinese-shoes>>. [Accessed 7 May 2013].
60. Villagran, L. (2011). Mexico's crime groups grabbing lucrative market for pirated goods. Available: <<http://www.bellinghamherald.com/2011/05/22/2025291/mexicos-crime-groups-grabbing.htm>>. [Accessed 7 May 2013].
61. O'Rourke, J. (2011). Fake detergent a new face on dirty money laundering. Available: <<http://www.theage.com.au/national/fake-detergent-a-new-face-on-dirty-money-laundering-20110430-1e1zp.html>>. [Accessed 7 May 2013].
62. Deckers Outdoor Corporation (2011). Customs Seizures and Raids Net More Than 400,000 Pairs of Fake Boots and Shoes. Press release, issued 10 January 2011.
63. García, C. R. A. (2010). Counterfeit Vuitton bags — distorted status symbol. Available: <http://www.koreatimes.co.kr/www/news/opinon/2010/12/137_78379.html>. [Accessed 8 May 2013].
64. Schmidle, N. (2010). Inside the Knockoff Tennis Shoe Factory. Available: <http://www.nytimes.com/2010/08/22/magazine/22fake-t.html?pagewanted=all&_r=0>. [Accessed 8 May 2013].
65. Havocscope [online]. (2013). Available from: <<http://www.havocscope.com/counterfeit-goods-ranking/>>. [Accessed 7 May 2013].
66. Villagran, L. (2011). Mexico's crime groups grabbing lucrative market for pirated goods. Available: <<http://www.dallasnews.com/news/20110516-mexicos-crime-groups-grabbing-lucrative-market-for-pirated-goods.ece>>. [Accessed 8 May 2013].
67. AAP. (2012). French luxury brands fight back against fakes. Available: <<http://www.news.com.au/business/companies/french-luxury-brands-fight-back-against-fakes/story-fnd1bsz-1226373273750>>. [Accessed 8 May 2013].
68. Sporting Goods Manufacturers Association [online]. (2011). Available from: <<http://www.sgia.org/publicpolicy/intellectualpropertyactiveissues/counterfeitsseizuresup>>. [Accessed 8 May 2013].
69. Financial Action Task Force, 2012. Financial Action Task Force . The FATF Recommendations, [Online]. Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf [Accessed 8 May 2013].
70. EuroScan (2003). Counterfeit 200 Euro Bank Notes. Press release, issued 6 May 2003.
71. Androulakis, I. (2007). RFID Banknotes. Available: <<http://www.fleur-de-coin.com/eurocoins/banknote-rfid>>. [Accessed 8 May 2013]

Drug Trafficking

1. United Nations Office on Drugs and Crime (UNODC) (2011). Estimating Illicit Financial Flows resulting from drug trafficking and other transnational organised crimes. Available at: <http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf>. [Accessed 9 May 2013].
2. United Nations Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <<http://www.unodc.org/documents/data-and-analysis/WDR2011/WDR2011-web.pdf>>. [Accessed 9 May 2013].
3. United Nations Office on Drugs and Crime (UNODC) (2009). World Drug Report 2009. Available at: <http://www.unodc.org/documents/wdr/WDR_2009/WDR2009_eng_web.pdf>. [Accessed 9 May 2013].
4. United Nations Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <<http://www.unodc.org/documents/data-and-analysis/WDR2011/WDR2011-web.pdf>>. [Accessed 9 May 2013].
5. United Nations Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <<http://www.unodc.org/documents/data-and-analysis/WDR2011/WDR2011-web.pdf>>. [Accessed 9 May 2013].
6. United Nations Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <<http://www.unodc.org/documents/data-and-analysis/WDR2011/WDR2011-web.pdf>>. [Accessed 9 May 2013].
7. United Nations Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <<http://www.unodc.org/documents/data-and-analysis/WDR2011/WDR2011-web.pdf>>. [Accessed 9 May 2013].
8. United Nations Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <<http://www.unodc.org/documents/data-and-analysis/WDR2011/WDR2011-web.pdf>>. [Accessed 9 May 2013].

9. United Nations Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <<http://www.unodc.org/documents/data-and-analysis/WDR2011/WDR2011-web.pdf>>. [Accessed 9 May 2013].
10. United Nations Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <<http://www.unodc.org/documents/data-and-analysis/WDR2011/WDR2011-web.pdf>>. [Accessed 9 May 2013].
11. UN General Assembly, 1962 Single Convention on Narcotic Drugs as amended by the 1972 Protocol amending the 1961 Single Convention on Narcotic Drugs, March 30, 1961, 18 UST 1407 / 520 UNTS 204 / 14 ILM 302 (1975), Available at: <http://www.unodc.org/pdf/convention_1961_en.pdf>. [Accessed 9 May 2013].
12. UN General Assembly, 1971 Convention on Psychotropic Substances, Dec 9, 1975, A/RES/3443, Available at: <http://www.unodc.org/pdf/convention_1971_en.pdf>. [Accessed 9 May 2013].
13. UN General Assembly, 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 20, 1988, U.N. Doc. E/CONF.82/15 / 28 ILM.493 (1989), Available at: <http://www.unodc.org/pdf/convention_1988_en.pdf>. [Accessed 9 May 2013].
14. United Nations Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <<http://www.unodc.org/documents/data-and-analysis/WDR2011/WDR2011-web.pdf>>. [Accessed 9 May 2013].
15. Center for Substance Abuse Treatment. Treatment for Stimulant Use Disorders. (1999), Treatment Improvement Protocol (TIP), Series, No. 33. Available from: <<http://www.ncbi.nlm.nih.gov/books/NBK64337/>>. [Accessed 9 May 2013].
16. Department of the Treasury Office of Foreign Assets Control, (2000) Executive Order 12978—Blocking Assets and Prohibiting Transactions with Significant Narcotics Traffickers, 65 FR 75628. Available from: <<http://www.treasury.gov/resource-center/sanctions/Documents/12978.pdf>>. [Accessed 9 May 2013].
17. United Nations Office on Drugs and Crime (UNODC) (2009). World Drug Report 2009. Available at: <http://www.unodc.org/documents/wdr/WDR_2009/WDR2009_eng_web.pdf>. [Accessed 9 May 2013].
18. United Nations Office on Drugs and Crime (UNODC) (2009). World Drug Report 2009. Available at: <http://www.unodc.org/documents/wdr/WDR_2009/WDR2009_eng_web.pdf>. [Accessed 9 May 2013].
19. United Nations Office on Drugs and Crime (UNODC) (2009). World Drug Report 2009. Available at: <http://www.unodc.org/documents/wdr/WDR_2009/WDR2009_eng_web.pdf>. [Accessed 9 May 2013].
20. Ko-lin, C, Zhang, S, (2007). The Chinese Connection: Cross-border Drug Trafficking between Myanmar and China, (Unpublished Paper), Available at: <<https://www.ncjrs.gov/pdffiles1/nij/grants/218254.pdf>>. [Accessed 9 May 2013].
21. Cook, C, (2007). Mexico's Drug Cartels: CRS Report for Congress, Washington D.C. Congressional Research Service, 14. Available at: <<http://www.fas.org/sgp/crs/row/RL34215.pdf>>. [Accessed 9 May 2013].
22. Casas-Zamora, K. (2009). Guatemala's How to Prevent a Failed State in our Midst, Available at: <<http://www.brookings.edu/research/opinions/2009/05/22-guatemala-casaszamora>>. [Accessed 9 May 2013].
23. Felbab-Brown, V. (2010). The West African Drug Trade in the Context of the Region's Illicit Economies and Poor Governance, Available at: <<http://www.brookings.edu/research/speeches/2010/10/14-africa-drug-trade-felbab-brown>>. [Accessed 9 May 2013].
24. UN Office on Drugs and Crime (UNODC) (2011). World Drug Report 2011. Available at: <http://www.unodc.org/documents/data-and-analysis/WDR2011/World_Drug_Report_2011_ebook.pdf>. [Accessed 9 May 2013].

Environmental Crime

1. Warren, C [online]. (2013). Available at: <<http://www.brainyquote.com/quotes/quotes/w/warrenchri298523.html>>. [Accessed 10 May 2013].
2. Zabarenko, D (2012). Follow the money to catch illegal loggers: World Bank, Reuters, Available at: <<http://www.reuters.com/article/2012/03/21/us-logging-money-idUSBRE82K00620120321>>. [Accessed 10 May 2013].
3. Environmental Crime: A threat to our future by the UNODOC Environmental Investigation Agency (2008) [online] Available at: <http://www.unodc.org/documents/NGO/EIA_Erocrime_report_0908_final_draft_low.pdf>. [Accessed 8 September 2013]
4. Green Carbon, Black Trade: Illegal Logging, Tax Fraud and Laundering in the World's Tropical Forests; by UN Environment Programme and Interpol (2012) [online] Available at: <<http://www.interpol.int/content/download/16108/122549/version/1/file/PR075%20Green%20carbon%20black%20trade.pdf>>. [Accessed 8 September 2013]
5. Environmental Crime: A threat to our future by the UNODOC Environmental Investigation Agency (2008) [online] Available at: <http://www.unodc.org/documents/NGO/EIA_Erocrime_report_0908_final_draft_low.pdf>. [Accessed 8 September 2013]
6. Green Carbon, Black Trade: Illegal Logging, Tax Fraud and Laundering in the World's Tropical Forests; by UN

Environment Programme and Interpol (2012) [online] Available at: <<http://www.interpol.int/content/download/16108/122549/version/1/file/PR075%20Green%20carbon%20black%20trade.pdf>> [Accessed 8 September 2013]

7. EU Organised Crime Threat Assessment: Europol (2011) [online] Available at: <http://www.europol.europa.eu/sites/default/files/publications/octa_2011.pdf> [Accessed 8 September 2013]
8. Environmental Crime: A threat to our future by the UNODC Environmental Investigation Agency (2008) [online] Available at: <http://www.unodc.org/documents/NGO/EIA_Erocrime_report_0908_final_draft_low.pdf> [Accessed 8 September 2013]
9. Operation Worthy: Interpol targeted criminal organisations behind the illegal trafficking of ivory which resulted in more than 200 arrests and the seizure of nearly two tons of contraband elephant ivory. The operation involved 14 countries across Eastern, Southern and Western Africa and resulted in the recovery of more than 20 kilos of rhinoceros horn in addition to lion, leopard and cheetah pelts, crocodile and python skins, live tropical birds, turtles, and other protected species destined to be illegally trafficked around the world. Firearms including AK-47s, G3s and M16s were also seized by law enforcement officers. More than 320 officers from a range of agencies including police, customs, environmental protection agencies, veterinary services, airport security, ministries of tourism and national prosecuting authorities took part in Operation Worthy which saw interventions carried out at markets, ports, shops, border crossings and during roadside checks.
10. UN Environment Programme: Illegal Trade in Ozone Depleting Substances (2006) [online] tbc
11. to be completed
12. Havocscope (2013) [online] Available at: <<http://www.havocscope.com/tag/illegal-fishing/>> [Accessed 8 September 2013]
13. Federation of American Scientists (online): International Crime Threat Assessment: states that, "Environmental crime is one of the most profitable and fastest growing new areas of international criminal activity. Growing international environmental concerns have led to the proliferation of multilateral conventions and national laws and regulations to control pollutants that are health or environmental hazards, to prevent wanton exploitation of scarce natural resources, and to protect endangered plant and animal species. Criminal organisations around the world--most notably in Italy, Russia, China, and Japan--have taken advantage of the significantly greater costs for waste disposal, as well as the much-increased value of rare or precious natural resource commodities that are the subject of tight trade and sale restrictions, to earn substantial illicit income from circumventing environmental laws and regulations. The US Government estimates that local and international crime syndicates worldwide earn \$22-31 billion annually from hazardous waste dumping, smuggling proscribed hazardous materials, and exploiting and trafficking protected natural resources. The tremendous costs for legally disposing of pollutants and dangerous chemicals have created new illicit business opportunities for criminal organisations, who earn \$10-12 billion per year for dumping trash and hazardous waste materials. Organised crime groups are taking increasing advantage of the multibillion-dollar legal trade in recyclable materials, such as scrap metals, to comingle or illegally export or dump toxic wastes. Most of these wastes are shipped in "trash-for-cash" schemes to countries in Eastern and Central Europe, Asia, and Africa where disposal costs and enforcement of environmental regulations are lower. The lack of specific legislation governing such crimes in many countries and poor enforcement or limited legal penalties in many others (often only fines that are insignificant in comparison to the millions in profits that can be made from this activity) reduce the risks for international crime groups involved in dumping hazardous wastes. While crime groups in Russia, Japan, and elsewhere have increasingly moved into illegal waste disposal, Italian criminal organisations are the most involved largely because of their success in infiltrating Italy's industrial waste disposal sector. They have used their control over waste-disposal businesses, both legitimate and front companies, to secure contracts in Italy and elsewhere in Europe and illegally dump wastes to boost profits. About half the 80 million metric tons of waste produced annually in Italy disappears and is presumed to be illegally dumped, according to Italian press sources. In 1997, Italian law enforcement authorities investigating the role of Italian organised crime in the illegal export and dumping of hazardous wastes claimed that criminal groups control most of Italy's waste disposal contracts. Italian authorities claimed in 1997 that 11 million metric tons of toxic and industrial waste are deposited annually in some 2,000 illegal domestic dump sites in local waterways or in the Mediterranean. In 1997, there were at least 53 Italian crime groups trafficking and disposing of hazardous waste, which was shipped to dumpsites in Albania, Eastern Europe, and the African west coast, according to European law enforcement officials cited in the press. The lack of inexpensive, adequate, safe disposal options for radioactive waste is also attracting the increased involvement of organised crime groups throughout Europe. In many cases, these groups appear to be using illicit networks already in place for smuggling arms, drugs, and other contraband. European authorities are investigating illegal dumping of radioactive wastes from Austria, France, and Germany--all of which have good, but costly, disposal options--and

Eastern Europe into the Mediterranean and Adriatic Seas by companies purportedly hired by Italian organised crime groups. In 1998, an 'Ndrangheta Italian organised crime family was being investigated by Italian authorities for dumping radioactive waste off Italy's southern coast, according to press reports." Available at:<<https://www.fas.org/irp/threat/pub45270chap2.html>> [Accessed on 8 September 2013]

14. Wikipedia [online]. (2013). Available at: http://en.wikipedia.org/wiki/Exxon_Valdez_oil_spill. [Accessed 10 May 2013].
15. UN Environment Programme (2006). Ecosystems and Biodiversity in Deep Waters on High Seas, UNEP Regional Seas Reports and Studies No 178 UNEP/IUCN, Switzerland 2006. ISBN 92-807-2734-6
16. Greenpeace Plastic Debris in the World's Oceans: (2006) [online] <http://www.unep.org/regionalseas/marinelitter/publications/docs/plastic_ocean_report.pdf> [Accessed 8 September 2013]
17. Sources: Marine Pollution: Progress Made to Reduce Marine Pollution by Cruise Ships, but Important Issues Remain (February 2000 -- Washington, DC: GAO), and various new reports
18. At Three Mile Island in 1979 the main water pumps feeding the cooling system of reactor 2 failed, which resulted in partial melting of the reactor core and a release of approximately one thousandth (1/1000),as much radiation as during the Chernobyl explosion. Debate about how close the reactor came to a complete melt down have been heated with advocates on both sides claiming both safety measures were sufficient and others that it was only down to luck that the core didn't totally collapse and a massive release of radiation ensue. A few days after the accident all children and pregnant women were evacuated from an 8 km radius of the plant as a safety precaution. Radiation from the plant reactor is thought to have contributed to the premature deaths of some elderly people that lived in the region. Dairy farmers reported that many animals have died consequential to the accident and local residents have developed cancers. The reactor cleanup started in 1979 and officially ended in 1993 at a cost of around US\$975mio.

Extortion

1. Rand, A [online]. (2013). Available at: <<http://www.goodreads.com/quotes/430626-to-count-upon-his-virtue-and-use-it-as-an>>. [Accessed 11 May 2013].
2. Malkin, E, (2011). As Gangs Move In on Mexico's Schools, Teachers Say 'Enough,' New York Times, Available at: <<http://www.havocscope.com/unreported-extortion-in-mexico/>>. [Accessed 11 May 2013].
3. Oren, M (2005). The Middle East and the Making of the US, 1776 to 1815. Speech delivered at Columbia University. Available at: <<http://www.columbia.edu/cu/news/05/11/michaelOren.html>>. [Accessed 11 May 2013].

Forgery

1. Malinowski, B [online]. (1942). Available at: <<http://www.brainyquote.com/quotes/quotes/b/bronislawm312106.html>>. [Accessed 12 May 2013].
2. Halsey III, A (2011). Latest counterfeit IDs are so good they're dangerous, Washington Post, July 30, 2011, Available at: <<http://www.havocscope.com/price-for-counterfeit-identifications-from-china/>>. [Accessed 12 May 2013].
3. Cairo,I [online]. (2008). Suriname seeks Interpol assistance in passports scam in Thailand, Available at: <http://www.caribbeannewsnow.com/caribnet/suriname.php?news_id=7792&start=440&category_id=36>. [Accessed 12 May 2013].

Fraud incl Tax Fraud & Cybercrime

1. Buffet, W [online] (2002) Available at: <<http://www.brainyquote.com/quotes/quotes/w/warrenbuff383933.html>>. [Accessed 13 May 2013].
2. Association of Certified Fraud Examiners, (1996) Report to the Nations on Occupational Fraud And Abuse, Available at: <http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/1996-rttn.pdf>. [Accessed 13 May 2013].
3. National Fraud Authority (2011) Annual Fraud Indicator, Available at: <<http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/annual-fraud-indicator-2011?view=Binary>>. [Accessed 13 May 2013].
4. Financial Services Authority [online]. (2013) Share fraud and boiler room scams. Available at: <http://www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams/boiler_room>. [Accessed 13 May 2013].
5. UN Office on Drugs and Crime (UNODC) Division for Policy Analysis and Public Affairs, Eighth UN Survey of Crime Trends and Operations of Criminal Justice Systems, covering the period 2001 – 2002, Available at <<http://www.unodc.org/pdf/crime/eighthsurvey/8sv.pdf>>. [Accessed 13 May 2013].

6. CSIS noted the difficulty of relying on methods such as surveys because companies that reveal their cyber losses often cannot estimate what has been taken, intellectual property losses are difficult to quantify and the self-selection process of surveys can distort the results. For purposes of the research, CSIS classified malicious cyber activity into the following areas: the loss of intellectual property; the loss of sensitive business information, including possible stock market manipulation; opportunity costs, including service disruptions and reduced trust for online activities; the additional cost of securing networks, insurance and recovery from cyber attacks and reputational damage to the hacked company. "We believe the CSIS report is the first to use actual economic modeling to build out the figures for the losses attributable to malicious cyber activity," said Mike Fey, executive vice president and chief technology officer at McAfee. Available at <<http://www.CSIS.org/press/press-release/csis-releases-first-study-connect-cyber-crime-job-loss>> [Accessed 8 September 2013]
7. Financial Action Task Force. [online]. (2012) Documents:- Laundering the Proceeds of VAT Carousel Fraud Report. Available at: <<http://www.fatf-gafi.org/topics/methodsandtrends/documents/launderingthe proceedsofvatcarouselfraudreport.html>>. [Accessed: 13 May 2013].
8. Further Key Findings from the report, "Illicit Financial Flows from China and the Role of Trade Misinvoicing" by Global Financial Integrity stated that: Mis-invoiced trade between Chinese companies and the US increased from US\$48.8bio in 2000 to US\$59.0bio in 2011. The volume of trade misinvoicing between mainland China and the US rose to US\$72.0 billion before the financial crisis of 2008, but has declined since then, probably as a result of lower growth in bilateral trade between the countries. The commodity groupings most susceptible to trade misinvoicing include nuclear reactors, boilers, machinery, etc. and electrical and electronic equipment, with the sub-group for electronic circuits showing the largest cumulative illicit outflows (US\$84.0bio). Trade misinvoicing related to the sub-group for mobile phones increased at the fastest pace from 2007-2011. Of the roughly US\$2.83 trillion that flowed illicitly out of China from 2005-2011, US\$595.8bio wound up as cash deposits or financial assets (such as stocks, bonds, mutual funds, and derivatives) in tax havens. Available at: (2012) [online] <<http://www.gfiintegrity.org/storage/gfip/documents/reports/ChinaOct2012/gfi-china-oct2012-report-web.pdf>>
9. The tax gap is defined as the amount of tax liability faced by taxpayers that is not paid on time. The US Internal Revenue Service collects more than US\$2 trillion annually in taxes so producing an estimate of the tax gap is a major statistical effort that it undertakes every few years. In 2012 the IRS released a new set of tax gap estimates for tax year 2006. The new tax gap estimate represents the first full update of the report in five years, and it shows the nation's compliance rate is essentially unchanged at about 83% from the last review covering tax year 2001, at around US\$385bio. US IRS (2012) [online] Available at <<http://www.irs.gov/uac/The-Tax-Gap>> [Accessed 8 September 2013]
10. Measuring the Size, Growth and Determinants of Income Tax Evasion in the U.S by Richard Cebula and Edgar L. Feige (2011) [online] Available at <<http://www.ssc.wisc.edu/econ/archive/wp2011-1.pdf>> [Accessed 8 September 2013]. This study empirically investigated the US tax gap and employing the most recent data they found that 18-19% of total reportable income is not properly reported to the IRS, giving rise to a "tax gap" approaching \$500 billion dollars.
11. US senators estimate of US tax gap
12. Europol (2009) [online] Available at: <<http://www.europol.europa.eu/content/press/carbon-credit-fraud-causes-more-5-billion-euros-damage-european-taxpayer-1265>> [Accessed 8 September 2013]
13. First Annual Cost of Cybercrime Study; Benchmark Study of US Companies sponsored by ArcSight, independently conducted by Ponemon Institute LLC (2010) [online] Available at: <http://www.hpcenterprisesecurity.com/collateral/report/HPEEnterpriseSecurity_Report_HPArcSightFirstAnnualCostCybercrimeStudyPonemon.pdf> [Accessed 8 September 2013]
14. Symantec Corp: Norton Cybercrime Report 2011 (2011) [online] Available at: <http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02> [Accessed 8 September 2013].
15. Sans Technology Institute (2013) [online] Available at: <<http://www.sans.edu/research/security-laboratory/article/security-predict2011>> [Accessed 8 September 2013]
16. Group IB: State and Crime of the Russian Digital Crime Market 2011 (2011) [online] Available at: <http://www.group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf> [Accessed 8 September 2013]
17. UK National Audit Office/cybercrime

Human Trafficking

1. UN Office on Drugs and Crime (UNODC). (2006). Trafficking in persons: Global patterns, Available at: <http://www.unodc.org/pdf/traffickinginpersons_report_2006ver2.pdf>. [Accessed 14 May 2013].
2. UN Office on Drugs and Crime (UNODC) (2010). Global report on trafficking in persons, Available at: <

- [http://www.unodc.org/documents/Global_Report_on_TIP.pdf

3. The UN estimates the total market value of illicit human trafficking at US\\$32bio \(ILO, 2005\) - \[online\] Available at <\[http://www.unodc.org/documents/human-trafficking/UNVT_Fs_HT_EN.pdf\]\(http://www.unodc.org/documents/human-trafficking/UNVT_Fs_HT_EN.pdf\)> \[Accessed 8 September 2013\]

4. Havocscope \[online\]. 2013 Available from <<http://www.havocscope.com/illicittrade/>> \[Accessed 14 July 2013\]

5. Ken Ellingwood, \(2004\). Hard Line: Life and Death on the US-Mexico border, \(New York: Pantheon\). Available at: <<http://www.havocscope.com/human-smuggler-usage-on-the-us-mexico-border/>>. \[Accessed 14 May 2013\].](http://www.unodc.org/documents/Global_Report_on_TIP.pdf)

Illicit Arms Trafficking

1. United States, (2012). UN Launches International Small Arms Control Standards with Aim. [press release] 30 August 2012, Available at: <<http://www.un.org/News/Press/docs/2012/dc3387.doc.htm>>. [Accessed 15 May 2013].
2. United Stations, (2012). UN Launches International Small Arms Control Standards with Aim. [press release] 30 August 2012, Available at: <<http://www.un.org/News/Press/docs/2012/dc3387.doc.htm>>. [Accessed 15 May 2013].
3. Small Arms Survey 2012. Cambridge University Press, DC/3387, Available at: <<http://www.smallarmssurvey.org/publications/by-type/yearbook/small-arms-survey-2012.html>>. [Accessed 15 May 2013].
4. The Small Arms Survey is an independent research project located at the Graduate Institute of International and Development Studies in Geneva, Switzerland. It provides impartial and public information on all aspects of small arms and light weapons, as a resource for governments, policy-makers, researchers, and activists, as well as research on small arms issues. The Survey monitors national and international initiatives (governmental and non-governmental), and acts as a forum and clearinghouse for the sharing of information. It also disseminates best practice measures and initiatives dealing with small arms issues. The Small Arms Survey mandate is to look at all aspects of small arms and armed violence. It provides research and analysis to support Governments to reduce the incidence of armed violence and illicit trafficking through our evidence-based analysis. Project staff includes international experts in security studies, political science, law, international public policy, development studies, economics, conflict resolution, and sociology. The staff works closely with a worldwide network of researchers and partners. Small Arms Survey (2013) [online] Available at: <<http://www.smallarmssurvey.org>> [Accessed 8 September 2013]
5. THE SECRETARY-GENERAL (1997). GENERAL AND COMPLETE DISARMAMENT: SMALL ARMS. Report of the Panel of Governmental Experts on Small Arms. [report]. Available at: <<http://www.un.org/Depts/ddar/Firstcom/SReport52/a52298.html>>. [Accessed 15 May 2013].

Insider Dealing

1. Wall Street (1987). [DVD] US: Oliver state.
2. Dienst, J. (2010). Preet Bharara Receives Award And Gives Speech At Fraud Conference. WNBC, [online] 21 October. Available at: <<http://www.nbcnewyork.com/news/local/Insider-Trading-Rampant-On-Wall-St-US-Attorney-105399138.html>>. [Accessed: 16 May 2013].
3. Updated Measurement of Market Cleanliness. 25. [report] London: Financial Services Authority. Available at: <<http://www.fsa.gov.uk/pubs/occapers/op25.pdf>>. [Accessed: 16 May 2013].
4. Committee on the Judiciary US Senate. (2013). Illegal Insider Trading: How widespread is the problem and is there adequate criminal enforcement?. J-109-117. [report] Washington: U.S. Government Printing Office. Available at: <<http://www.gpo.gov/fdsys/pkg/CHRG-109shrg31445/pdf/CHRG-109shrg31445.pdf>>. [Accessed: 16 May 2013].
5. Hennesse Group (2013). Hedge Funds increase use of credit derivatives. [press release] October 30 2006. Available at: <<http://www.hennessegroup.com/releases/release20061030.html>>. [Accessed: 16 May 2013].
6. Ashe, M. and Counsell, L. (2000). Market Abuse - The crime of being something in the City. NLJ, 1344 (1), Available at: <http://www.9stonebuildings.com/publications/market_abuse.pdf>. [Accessed:16 May 2013].
7. FSA handbook info. [online] (2001). Code of Market Conduct. Available at: <<http://fsahandbook.info/FSA/html/handbook/MAR/1>>. [Accessed: 16 May 2013].
8. International Organisation of Securities Commissions. [online] (2003). Objectives and principles of securities regulation. Available at: <<http://www.iosco.org/library/pubdocs/pdf/IOSCOPD154.pdf>>. [Accessed:16 May 2013].
9. FINMA. (2003). Marker conduct rules for the securities. [online] Available at: <<http://www.finma.ch/e/regulierung/Documents/finma-rs-2008-38-e.pdf>>. [Accessed: 16 May 2013].

Kidnap, Illegal Restraint & Hostage Taking

1. Schmidle, N. (2009). The Hostage Business. The New York Times, 4 December. Available at: <http://www.nytimes.com/2009/12/06/magazine/06kidnapping-t.html?pagewanted=all&_r=0>. [Accessed 17 May 2013].
2. Chaudhry, I. (2012). January to March 2012 kidnapping for ransom cases in Lahore. Daily Times, 23 March. Available at: <<http://www.havocscope.com/january-to-march-2012-kidnapping-for-ransom-cases-in-lahore/>>. [Accessed 17 May 2013].
3. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf. [Accessed 17 May 2013].
4. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: <https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf>. [Accessed 17 May 2013].
5. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: <https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf>. [Accessed 17 May 2013].
6. Financial Action Task Force (2011). Organised Maritime Piracy and Related Kidnapping for Ransom. [report]. Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/organised%20maritime%20piracy%20and%20related%20kidnapping%20for%20ransom.pdf>>. [Accessed 17 May 2013].
7. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: <https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf>. [Accessed 17 May 2013].
8. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: <https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf>. [Accessed 17 May 2013].
9. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: <https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf>. [Accessed 17 May 2013].
10. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: <https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf>. [Accessed 17 May 2013].
11. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: <https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf>. [Accessed 17 May 2013].
12. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: <https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf>. [Accessed 17 May 2013].
13. Red 24 [online]. (2012). Top 10 Kidnap Countries Named By Red 24. Available at: <https://www.red24.com/uploads/crm/top10kidnapcountriesbyred24_02042012.pdf>. [Accessed 17 May 2013].
14. Financial Action Task Force (2011). Organised Maritime Piracy and Related Kidnapping for Ransom. [report]. Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/organised%20maritime%20piracy%20and%20related%20kidnapping%20for%20ransom.pdf>>. [Accessed 17 May 2013].
15. Source: "Hostage-taking: Trading places," The Economist, March 16, 2013.
16. Source: Adam Nossiter, "Millions in Ransoms Fuel Militants' Clout in West Africa," New York Times, December 12, 2012.
17. Source: <http://www.belfasttelegraph.co.uk/news/g8-summit/g8-leaders-agree-to-stamp-out-terrorist-ransoms-29353978.html>
18. Wiese Bockmann, M. [online] (2012). Somali Pirates Cost \$6.9B as Attacks Reach Record. Bloomberg, 8 February. Available at: <<http://www.havocscope.com/average-ransom-demand-by-pirates-in-somalia-in-2011/>>. [Accessed 17 May 2013].
19. Financial Action Task Force (2011). Organised Maritime Piracy and Related Kidnapping for Ransom. [report]. Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/organised%20maritime%20piracy%20and%20related%20kidnapping%20for%20ransom.pdf>>. [Accessed 17 May 2013].
20. Walsh, D. [online]. (2012). Taliban Gaining More Resources From Kidnapping. The New York Times, 19 Feb. Available at: <http://www.nytimes.com/2012/02/20/world/asia/pakistani-taliban-turn-to-kidnapping-to-finance-operations.html?pagewanted=all&_r=0>. [Accessed: 17 May 2013].
21. Adriano, J. [online]. (2012). To be abducted in the Philippines. Asia Times, 10 Feb. Available at: <http://www.atimes.com/atimes/Southeast_Asia/NB10Ae02.html>. [Accessed 17 May 2013].
- 22..Mcavoy , E. [online]. (2010). The £1 billion hostage trade. Independent, 17 October. Available at: <<http://www.independent.co.uk/news/world/politics/the-1-billion-hostage-trade-2108947.html>>. [Accessed 17 May].
23. Financial Action Task Force (2011). Organised Maritime Piracy and Related Kidnapping for Ransom. [report]. Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/organised%20maritime%20piracy%20and%20related%20kidnapping%20for%20ransom.pdf>>. [Accessed 17 May 2013].
24. <http://www.theguardian.com/tv-and-radio/tvandradioblog/2012/feb/23/hostage-negotiator-kidnap-and-ransom-reality-check>

Market Manipulation

1. Condon, B., Freedman, M. and Karmali, N. (2005). Facing brutal competition in the U.S., giant Citigroup is reaching out to the burgeoning middle classes around the world. Forbes, [online] 18 April. Available at: <http://www.forbes.com/free_forbes/2005/0418/068.html>. [Accessed: 17 May 2013].
2. The Financial Crisis Inquiry Commission. (2011). The Financial Crisis Inquiry Report. [report]. Available at: <<http://www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf>>. [Accessed: 17 May 2013].
3. FSA handbook info. [online] (2001). Code of Market Conduct. Available at: <<http://fsahandbook.info/FSA/html/handbook/MAR/1>>. [Accessed: 17 May 2013].
4. Financial Action Task Force (2009) Money laundering and terrorist financing in the securities sector. Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf>>. [Accessed: 17 May 2013].

Murder & Previous Bodily Injury

1. International Federation of Journalists (2010). Gunning for Media Journalists and Media Staff Killed in 2010. [report] Belgium: International Federation of Journalists International Press Centre. Available at: <<http://www.ifj.org/assets/docs/177/154/f8badb1-b93699a.pdf>>. [Accessed 18 May 2013]
2. Geneva Declaration (2013). Global Burden of Armed Violence. [report] Geneva Declaration Secretariat, Available at: <<http://www.genevadeclaration.org/fileadmin/docs/Global-Burden-of-Armed-Violence-full-report.pdf>>. [Accessed 18 May 2013].
3. UN Office on Drugs and Crime (UNODC). (2011). 2011 Global Study on Homicide, Available at: <http://www.unodc.org/documents/dataanalysis/statistics/Homicide/Global_study_on_homicide_2011_web.pdf>. [Accessed 18 May 2013].
4. UN Office on Drugs and Crime (UNODC). (2011). International Homicide Statistics (IHS) Available at: <<http://www.unodc.org/documents/data-and-analysis/IHS-rates-05012009.pdf>>. [Accessed 18 May 2013].

Organised Crime

1. UN Office on Drugs and Crime (UNODC). (2010) Organised Crime Has Globalized and Turned into a Security Threat. [press release]. Available at: <<http://www.unodc.org/unodc/en/press/releases/2010/June/organized-crime-has-globalized-and-turned-into-a-security-threat.html>>. [Accessed 20 May 2013].
2. UN Office on Drugs and Crime (UNODC) (2011). Estimating Illicit Financial Flows resulting from drug trafficking and other transnational organised crimes. Available at: <http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf>. [Accessed 20 May 2013].
3. UN Convention against transnational organised crime, (2000). 40 ILM 335 (2001) / UN Doc. A/55/383 at 25 (2000) / [2004] ATS 12 Available at: <http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf>. [Accessed 20 May 2013].
4. Wikipedia [online]. (2013) National Geographic. Available at: <http://en.wikipedia.org/wiki/National_Geographic>. [Accessed 20 May 2013]

Smuggling

1. Famousquotes.com [online]. (2011). Brian Moskowitz Quotes | Famous Brian Moskowitz Quotations. Available at: <http://www.famousquotes.com/author/brian-moskowitz>. [Accessed: 21 May 2013].
2. Nagy, J. (n.d.) Tackling cigarette smuggling with enforcement: World Customs Journal, 6 (2), Available at: <<http://www.worldcustomsjournal.org/media/wcj/-/2012/2/Nagy.pdf>>. [Accessed 21 May 2013].
3. Havocscope [online]. (n.d.) Financial Value of Criminal Activities. Available at: <<http://www.havocscope.com/products/ranking/>>. [Accessed 21 May 2013].
4. Murdock, H. [online]. (2012). In Niger Delta, Black-Market Oil Booms. Voice of America, 28 June. Available at: <http://www.voanews.com/content/nigeria_bunkering_niger_delta_oil_market/1337346.html>. [Accessed 21 May 2013].
5. Unknown. [online]. (2012) Black gold on the black market. The Economist, 4 August. Available at: <<http://www.economist.com/node/21559962>>. [Accessed 21 May 2013].
6. Havocscope (n.d.) [online]. Gas and Oil Smuggling by Market., Available at: <<http://www.havocscope.com/gas-and-oil-smuggling-by-markets>>. [Accessed 21 May 2013].
7. Seifman, D. [online]. (2012) Counterfeit Tax Stamps in New York City. New York Post, June 8. Available at: <http://www.nypost.com/p/news/local/cig_tax_cheating_stores_burn_city_luuaDIHR0g99Wj1qpBntuK>. [Accessed 21 May 2013].

8. Thaffe, N. [online]. (2012). Government losing US\$bio in illicit tobacco trade. The Gleaner, 8 June. Available at: <<http://jamaica-gleaner.com/gleaner/20120608/lead/lead4.html>>. [Accessed 21 May 2013].
9. Europol Public Information (2011).EU Organised Crime Threat Assessment , OCTA 2011. [report] p.30 Available at: <http://migrantsatsea.files.wordpress.com/2011/05/octa_2011-1.pdf>. [Accessed 21 May 2013].
10. Havocscope (n.d.) Price List of Endangered Animals. [online] Available at: <<http://www.havocscope.com/black-market-prices/endangered-animals/>>. [Accessed 21 May 2013].
11. Unknown.(2011). 'Growing problem' of illegally distilled alcohol . BBC News, [online] 14 July. Available at: <<http://www.bbc.co.uk/news/uk-england-14151509>>. [Accessed 21 May 2013].
12. Bennion, J. [online]. (2007). Iraq: The Alcohol Smugglers. Frontline World, 20 August. Available at: <http://www.pbs.org/frontlineworld/rough/2007/08/iraq_the_alcohol.html#>. [Accessed 21 May 2013].
13. ARA, Ilicit and Non-Commercial Alcohol, Industry Association for Responsible Alcohol Use, Available at: <<http://www.havocscope.com/alcohol-smuggling-in-canada/>>. [Accessed 21 May 2013].
14. Havocscope - The Black Market Economy [online]. (2013). Available from: <<http://www.havocscope.com/alcohol-smuggling-market-value/>>. [Accessed 21 May 2013].
15. Haken, J [online]. (2011). Transnational Crime in the Developing World. Global Financial Integrity, 1 February. Available at: <http://www.gfiintegrity.org/storage/gfip/documents/reports/transcrime/gfi_transnational_crime_web.pdf>. [Accessed 21 May 2013].
16. Unknown.[online]. (2013). Gold and guerillas. The Economist, 17 August. Available at: <<http://www.economist.com/blogs/americasview/2012/08/mining-colombia>>. [Accessed 21 May 2013].
17. Fox, E. [online]. (2012) FARC Set to Exploit Venezuela 'Conflict Mineral'. In Sight Crime, [online] 12 March. Available at: <<http://www.insightcrime.org/news-analysis/farc-set-to-exploit-venezuela-conflict-mineral>>. [Accessed 21 May 2013].
18. Thakur, P. (2012). Conflict diamonds' entry to India raises money laundering fear. The Times Of India, [online], 26 June. Available at: <http://articles.timesofindia.indiatimes.com/2012-06-26/india/32423440_1_conflict-diamonds-kimberley-process-certification-rough-diamonds>. [Accessed 21 May 2013].
19. The Associated Press. (2009) US Says Refineries Bought Oil Smuggled From Mexico. The New York Times, [online] 10 August. Available at: <http://www.nytimes.com/2009/08/11/business/energy-environment/11oil.html?_r=1&>> [Accessed 21 May 2013].
20. <<http://www.eluniversal.com.mx/notas/618515.html>>
21. Financial Action Task Force (2012). Illicit Tobacco Trade. [report]. Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/Illicit%20Tobacco%20Trade.pdf>>. [Accessed 22 May 2013].
22. Wikipedia [online] (2012). Wildlife smuggling Available at: <http://en.wikipedia.org/wiki/Wildlife_smuggling#cite_note-1>. [Accessed 22 May 2013].
23. Wikipedia [online] (2012). Wildlife smuggling Available at: <http://en.wikipedia.org/wiki/Wildlife_smuggling#cite_note-1>. [Accessed 22 May 2013].
24. Walker, G. [online]. (2011). Illicit tobacco sales fall while beer rises," The Grocer, 29 September. Available at: <<http://www.havocscope.com/beer-smuggling-sales-in-the-united-kingdom/>>. [Accessed 22 May 2013].
25. Financial Action Task Force (2010). International Best Practices detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments. Available at: <http://www.coe.int/t/dghl/monitoring/moneyval/web_ressources/FATF_BPSRIX.pdf>. [Accessed 22 May 2013].

Terrorism Finance

1. Harnden, T. (2013). We'll starve the murderers of cash, says Bush. The Telegraph, [online] 25 Sep. Available at: <<http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1341569/Well-starve-the-murderers-of-cash-says-Bush.html>>. [Accessed 23 May 2013].
2. Ashley, P. (2012). The complete encyclopedia of terrorist organisations. Philadelphia, PA: Casemate.
3. Maplecroft [online]. (2011). Newly formed South Sudan joins Somalia, Pakistan, Iraq and Afghanistan at top of Maplecroft terrorism ranking. Available at: <http://maplecroft.com/about/news/terrorism_index_2011.html>. [Accessed 23 May 2013].
4. Maplecroft [online]. (2011). Maplecroft terrorism ranking – attacks up 15% globally. Available at: <http://maplecroft.com/about/news/terrorism_index_2011.html>. [Accessed 23 May 2013].
5. Global Terrorism Database . [online] (n.d.) Information on Over 104,000 Terrorist Attacks. Available at: <<http://www.start.umd.edu/gtd/>>. [Accessed 23 May 2013].
6. Terrorist Financing Staff Monograph (n.d.) Al-Qaeda's Means and Methods to Raise, Move, and. [online] Available at: <http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Ch2.pdf>. [Accessed 23 May 2013].

7. Wikipedia [online]. (2012). History of terrorism. Available at: <http://en.wikipedia.org/wiki/History_of_terrorism#cite_note-8>. [Accessed 23May 2013].
8. Wikipedia [online]. (2012). History of terrorism. Available at: <http://en.wikipedia.org/wiki/History_of_terrorism#cite_note-8>. [Accessed 23 May 2013].
9. Wikipedia [online]. (2012). History of terrorism. Available at: <http://en.wikipedia.org/wiki/History_of_terrorism#cite_note-8>. [Accessed 23 May 2013].
10. Wikipedia [online]. (2012). History of terrorism. Available at: <http://en.wikipedia.org/wiki/History_of_terrorism#cite_note-8>. [Accessed 23 May 2013].
11. UN . 1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft, ICAO Doc. 8364/704 UNTS 220/[1970] ATS 14/2 ILM 1042 (1963) / [Accessed 23 May 2013].
12. UN, Convention for the Suppression of Unlawful Seizure of Aircraft, 16 December 1970, UN Treaty Series 1973,
13. International Civil Aviation Organisation (ICAO), Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 23 September 1971, 974 UNTS 177,
14. UN, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 24 February 1988, UN Treaty Series 1990.
15. UN General Assembly, Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 10 March 1988, No. 29004,
16. UN General Assembly, Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, 10 March 1988, UNTS 1678, I-29004,
17. UN General Assembly, International Convention for the Suppression of the Financing of Terrorism, 9 December 1999, No. 38349,
18. UN General Assembly, International Convention for the Suppression of the Financing of Terrorism, 9 December 1999, No. 38349,

Theft Robbery and Trafficking

1. Juvenal,D, [online] (n.d.) Available at: <http://www.searchquotes.com/quotation/A_man_who_has_nothing_can_whistle_in_a_robber_s_face/241276/>. [Accessed 24 May 2013].
2. UN Office on Drugs and Crime (UNODC) (2010) World Report 2010. Available at: <http://www.unodc.org/documents/wdr/WDR_2010/World_Drug_Report_2010_lo-res.pdf>. [Accessed 24 May 2013].
3. UN Office on Drugs and Crime (UNODC) (2010) World Report 2010. Available at: <http://www.unodc.org/documents/wdr/WDR_2010/World_Drug_Report_2010_lo-res.pdf>. [Accessed 24 May 2013].
4. UN Office on Drugs and Crime (UNODC). (2010). The Globalization of Crime. A Transnational Organised Crime Threat Assessment. Available at:<http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf>. [Accessed 24May 2013].
5. Centre for Retail Research (2011). The Global Retail Theft Barometer 2011, Available at: <http://www.retailresearch.org/grtb_currentsurvey.php>. [Accessed 24 May 2013].
6. Frater, J [online]. (2009). <Available at: <http://listverse.com/2009/12/01/10-largest-robberies-in-history/#comments>>. [Accessed 24May 2013].
7. The Great Train robbery itself was a well planned and largely well executed endeavour. The train was brought to a halt at the isolated Railway Bridge by covering the line's green signal and attaching a battery to power its red light. All telephone lines within the local area had been cut to prevent an alarm being raised; therefore when a member of the train crew attempted to call the signalman he was unable to make a connection. This was the point at which the gang chose to reveal themselves, with members focussing their attack on the High Value Packages (HVP) carriage. Planning had gone as far as to designate one member with the task of familiarizing themselves with contemporary train operating controls, in order that the gang could uncouple the front carriage of the locomotive and drive it to an appropriate point to transfer the money to their vehicle. In the event gang members forced the train's original driver to do this, however the foresight to train one member in locomotive operation demonstrates the detail to which planning was undertaken. After loading 121 sacks containing bank notes into their waiting vehicle, the gang used back roads to make their way to a rural safe house. Along the way the group gathered valuable intelligence on police activity from radio broadcasts, monitoring police radio channels on a VHF radio. After lying low for several days the group dispersed from the farmhouse, which was to be cleaned of all potential traces of evidence by Brian Field. However this aspect of the plan proved to be a crucial sticking point, with Field failing to carry out this duty completely. As a result crucial evidence remained and was discovered by police before the gang could

return to complete the task of destroying any traceable evidence. In particular a fingerprint matching that of Roy James, the group's getaway driver, was found by police. Though ultimately unsuccessful for all known members of the group (three members are believed to have never been found), the heist has achieved somewhat iconic status, inspiring films such as *Buster* (based on the life of Ronald "Buster" Edwards). Particularly noteworthy is the story of Ronnie Biggs's life following the robbery. After serving 15 months of a 30 year sentence Biggs managed to flee to Paris, where he underwent plastic surgery and adopted a new identity with forged papers. Biggs then moved on to Adelaide, Australia, leading a quiet life as a builder. After tip off's that the police net was closing in about him, Biggs moved first to Melbourne and later onto Brazil where no extradition agreement existed with Britain. In Brazil Biggs fathered a son, rendering his legal protection from British extradition complete. As a result Biggs lived freely in Brazil for many years, however following three strokes he returned to the UK aged 71. Biggs then served 8 years of his sentence before being released on 'compassionate grounds' after a severe case of pneumonia. Today Ronnie Biggs has his own website and twitter account, through which he promotes his autobiography *Odd Man Out: The Last Straw*.

WMD Proliferation Finance

1. Bruton, J [online]. (n.d.) Available at: <http://www.searchquotes.com/quotation/Proliferation_of_nuclear_weapons_to_terrorist_organisations_is_far_more_dangerous_than_proliferation/90932/>. [Accessed 25 May 2013].
2. ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS [online]. (n.d.). History of the Chemical Weapons Convention. Available at: <<http://www.opcw.org/news-publications/publications/history-of-the-chemical-weapons-convention/>>. [Accessed 25 May 2013].
3. BBC [online]. (2013). BBC - WW2 People's War - Timeline. Available at: <<http://www.bbc.co.uk/history/ww2peopleswar/timeline/factfiles/nonflash/a6652262.shtml>>. [Accessed 25 May 2013].
4. Everything.Explained.At [online]. (1988). Halabja poison gas attack explained. Available at: <http://everything.explained.at/Halabja_poison_gas_attack/>. [Accessed 25 May 2013].
5. IAEA Illicit Trafficking Database, Fact Sheet [online]. (2008) International Atomic Energy Agency. Available at: <http://www.iaea.org/newscenter/features/radsources/pdf/fact_figures2007.pdf>. [Accessed 25 May 2013].
6. Financial Action Task Force [online]. (2008). PROLIFERATION FINANCING REPORT. Available at: <<http://www.fatfgafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>> [Accessed 23 May 2013].
7. AGA, C. [online]. (2013). Top 10 Countries with Nuclear Weapons. Available at: <<http://www.buzzle.com/articles/top10-nuclear-weapons-countries.html>>. [Accessed 25 May 2013].
8. ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS [online]. (n.d.) Global Campaign to Destroy Chemical Weapons Passes 60% Mark. Available at: <<http://www.opcw.org/nc/news/article/global-campaign-to-destroy-chemical-weapons-passes-60-percent-mark/>>. [Accessed 23 May 2013].
9. ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS [online]. (n.d.) Demilitarisation. Available at: <<http://www.opcw.org/our-work/demilitarisation/>>. [Accessed 23 May 2013].
10. Wikipedia [online]. (1992). Chemical Weapons Convention. Available at: <http://en.wikipedia.org/wiki/Chemical_Weapons_Convention#cite_note-CSP16-13>. [Accessed 23 May 2013].
11. Wikipedia [online]. (1939). Biological warfare. Available at: <http://en.wikipedia.org/wiki/Biological_warfare#United_Kingdom>. [Accessed 23 May 2013].
12. ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS [online]. (n.d.). History of the Chemical Weapons Convention. Available at: <<http://www.opcw.org/news-publications/publications/history-of-the-chemical-weapons-convention/>>. [Accessed 23 May 2013].
13. Wikipedia [online]. (1945). Atomic bombings of Hiroshima and Nagasaki. Available at: <http://en.wikipedia.org/wiki/Atomic_bombings_of_Hiroshima_and_Nagasaki>. [Accessed 23 May 2013].
14. UN Office for Disarmament Affairs [online]. (1963). UNODA - Non-Proliferation of Nuclear Weapons (NPT). Available at: <<http://www.un.org/disarmament/WMD/Nuclear/NPTtext.shtml>>. [Accessed 23 May 2013].
15. Arms control [online]. (2013). Nuclear Weapons: Who Has What at a Glance | Arms Control Association. Available at: <<http://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat>>. [Accessed 23 May 2013].
16. Wikipedia [online]. (2011). Sarin gas attack on the Tokyo subway - Wikipedia, the free encyclopedia. Available at: <http://en.wikipedia.org/wiki/Sarin_gas_attack_on_the_Tokyo_subway>. [Accessed 23 May 2013].
17. Suskind, R. (2006) *The one percent doctrine*. New York: Simon & Schuster
18. Graham, B. and others..(2013). World At Risk, The Report of the Commission on the Prevention. [e-book] US: Random House. Available at: <<http://a.abcnews.go.com/images/TheLaw/WMD-report.pdf#http://a.abcnews.go.com/images/TheLaw/WMD-report.pdf>>. [Accessed 23 May 2013].
19. The Guardian (2013) [online]: Available at: <<http://www.theguardian.com/world/2013/sep/02/syria-crisis>>

french-intelligence-assad> [Accessed 8 September 2013]

Part 1, Section 2, Sub-section 2 Customer Risks

1. Lord of War 2005. [film] Andrew Niccol. US: Lions Gate Films.
2. Shah, Anup. 2013. 'World Military Spending' Global Issues: Social, Political And Environmental Issues that Affect Us All. [online] Available at: <<http://www.globalissues.org/article/75/world-military-spending#worldmilitaryspending>>. [Accessed 14 July 2013]
3. Havocscope: Global Market Information. 2013. 'Value of Trafficking in Small Arms and Light Weapons' [online] Available at: <<http://www.havocscope.com/value-of-trafficking-in-small-arms-and-light-weapons/>> [Accessed 14 July 2013]
4. Stockholm International Peace Research Institute. 2011. 'The 15 Countries with the highest military expenditure in 2011' [online] Available at: <http://www.sipri.org/research/armaments/milex/resultoutput/milex_15/the-15-countries-with-the-highest-military-expenditure-in-2011-table/view> [Accessed 14 July 2013]
5. Stockholm International Peace Research Institute. 2009. 'Arms Transfers Database' [online] Available at: <<http://armstrade.sipri.org/armstrade/page/toplist.php>> [Accessed 14 July 2013]
6. Control Arms for example is a global civil society alliance campaigning for "a bulletproof Arms Trade Treaty" [online] Available at: <<http://www.controlarms.org>> [Accessed 6 September 2013]
7. Financial Action Task Force (FATF). 2012. 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations ('40 Recommendations)' [online] Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> [Accessed 14 July 2013]
8. Kindt, J. W. 2005. 'Gambling Quotes' [online] Available at: <http://www.casinowatch.org/john_kindt/kindt_quotes.html> [Accessed 14 July 2013]
9. Financial Action Task Force. 2009. 'Vulnerabilities of Casinos and Gaming Sector' [pdf]. [online] Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf>> [Accessed 14 July 2013]
10. PricewaterhouseCoopers. 2013. 'Playing to Win' [pdf] [online] Available at: <http://www.pwc.se/en_GX/gx/entertainment-media/pdf/pwc-playing-to-win.pdf> [Accessed 14 July 2013]
11. Havocscope: Global Black Market Information. 2013. 'Amount Illegally Wagered Worldwide' [online] Available at: <<http://www.havocscope.com/amount-illegally-wagered-worldwide/>> [Accessed 14 July 2013]
12. While there are casinos in many places, none have quite the long history or have defined a place more than the casino in Monte Carlo, in the Principality of Monaco. In 1850s the reigning Monaco's family was almost bankrupt and in a desperate bid to avert current decline began its transformation along lines which had seen success in German towns such as Baden-Baden, Wiesbaden and Homburg, namely focussing on become a resort location and in particular by setting up a casino. In the beginning Monaco's gambling enterprise was not successful as it was hard to reach both by land and by sea. After numerous owners, the casino passed into the hands of twin brothers Francois and Louis Blanc in 1863, for US\$1.7mio, who through gambling and speculating in stocks, via inside information and corruption had made enough money to first open a gambling business in Homburg in Germany, which became the most popular gambling resort in Europe. Under the brothers leadership, the casino in Monaco was lavishly decorated and new hotels and villas were built. A railway connection and increased ferry services connected Monaco to the rest of Europe. The Casino was located in a town in Monaco called "Les Spelugues" which meant "a den of thieves" and so this was changed to commemorate the then Prince Charles, renaming Les Spelugues as "Monte Carlo" – "Mount Charles". In the next 30 years the progress of Monaco was little short of marvelous thanks to grandiose success of Casino Monte Carlo. The number of hotels in the Principality grew from 2 to 48. The number of jewelers and florists increased from 3 to 15 and from 1 to 15 respectively. In 1900 there were 85 wine merchants against 17 in 1870. The service and retail industries went through a prolonged boom. The Opera house and the famous Oceanographic Museum were established. At the end of the 19th century almost a million tourists were visiting annually Monaco and casino Monte Carlo, when in 1850s the number was less than 200. Monte Carlo became a favorite playground and gambling Mecca for players, aristocracy and members of the Royal families, self-made millionaires and great artists. Whilst the casino continues to be successful, a gambler, Charles Wells was able to "break the bank" on two separate occasions, winning very large amounts in 1891 playing roulette. He played numbers lower than 10 and pocketed 1,000,000 gold francs. Song-writers in London wrote a song called "The Man who Broke the Bank in Monte-Carlo". On his return, he bet on number 5 and left with 3,000,000 francs. He was later convicted of cheating in another matter and would be imprisoned but the mystery of his amazing success in Monte Carlo was never revealed. In 1931, the casino introduced slot machines, which had become popular in the

US to go alongside the traditional gambling tables.

13. Changping, L. 2009. 'Casino King Entangled with Huang Guangyu' [online] Available at: <<http://english.caijing.com.cn/2009-01-09/110046571.html>> [Accessed 14 July 2013]
14. Collinson, P. 2011. 'Macau: where China likes to spend it' The Guardian Online, 5 March 2011. [online] Available at: <<http://www.guardian.co.uk/money/2011/mar/05/macau-china-spend>> [Accessed 14 July 2013]
15. Macau Daily Times. 2013. 'Criminal cases up by 10%' [online] Available at: <<http://macaudailytimes.com.mo/macau/30580-criminal-cases-percent.html>> [Accessed 14 July 2013]
16. Eadington, W. R. and Wang, W. 2007. 'VIP-room Contractual System of Macau's Traditional Casino Industry' [pdf] [online] Available at: <<http://business.unr.edu/econ/wp/papers/unreconwp07001.pdf>> [Accessed 14 July 2013]
17. Spectrum Gaming Group. 2010. 'White Paper: Indian Gambling Developments in International Jurisdictions: Insights for Indian Nations' [online] Available at: <<http://www.indiangaming.org/info/alerts/Spectrum-Internet-Paper.pdf>> [Accessed 14 July 2013]
18. OnlineGambling.com. 2013. 'The History of Online Gambling' [online] Available at: <<http://www.onlinegambling.com/online-gambling-history.htm>> [Accessed 14 July 2013]
19. US GAO Report 2002 [online] Available at: <<http://www.gao.gov/new.items/d0389.pdf>> (Accessed 8 September 2013)
20. Australian Government. 2000. Interactive Gambling (Moratorium) Act 2000. [online] Available at: <<http://www.comlaw.gov.au/Details/C2004C01150>> [Accessed 14 July 2013]
21. CIA Report on NGOs With Terror Links: 1996 (online) Available at: <http://en.wikisource.org/wiki/CIA_Report_on_NGOs_With_Terror_Links> Accessed 14 April 2013. According to wikileaks the 1996 CIA report stated as follows: International Islamic charities have established a presence in nearly every country around the world that has a substantial Muslim population. For both traditional and more activist Muslims, aiding Muslims in distress is a religious duty. Islamic activists dominate the leadership of the largest charities, and prominent members of some smaller organisations have been identified as extremists. The main objectives of these organisations include proselytizing, helping the needy, and defending Muslim communities from enemies. Where Muslims are engaged in armed conflict, some Islamic organisations provide military aid as part of a "humanitarian" package. The main Islamic charities maintain headquarters and raise money in a few regional centers, the most important being in the Arabian Peninsula and Sudan. Smaller organisations — important because of their support to extremist groups — often have headquarters in Europe and offices in North America. Private donors retain a major influence on each group's policies. Governments in the Islamic world generally support the major charities' religious activities and finance them, but are unable to monitor the groups or control how they use their money. These governments rely on the NGOs to collect and distribute much of the humanitarian aid given to refugees and displaced persons. Leaders of countries where Islamic NGOs are based or operate are unlikely to take major steps to stop the organisations' activities unless they believe that these groups threaten their own stability or are damaging important bilateral or multilateral relationships. All of the major and most of the minor Islamic charities are significant players in the former Yugoslavia, particularly in aiding Bosnian Muslims. Their contributions represent a significant proportion of humanitarian aid in Bosnia. According to the US embassy in Riyadh, Saudi nationals alone gave \$150 million through Islamic NGOs for aid to Bosnia in 1994. Most of the offices of NGOs active in Bosnia are located in Zagreb, Sarajevo, Zenica, and Tuzla. Their field operations appear to be confined to the Muslim areas of Northeastern and Central Bosnia. The NGOs' charitable activities include delivery of food, clothing, and medicine; support to orphanages, schools, hospitals, and refugee camps; and housing construction, infrastructure support, and agricultural projects. Many of these organisations also support foreign Mujahideen fighters in Bosnia. Coordination councils based in Zagreb and Sarajevo, coordinate the activities of the most important organisations. These councils may function like a similar one established in Peshawar, Pakistan, which organises arms shipments and aid to military training camps, and provides humanitarian aid to refugees, according to a clandestine source. A growing body of reporting indicates that some of these charities are being used to aid Islamic extremist groups that engage in terrorism. We have information that nearly one third of the Islamic NGOs in the Balkans have facilitated the activities of Islamic groups that engage in terrorism, including the Egyptian Al-Gama'at Al-Islamiyya, Palestinian Hamas, Algerian Groups, and Lebanese Hezbollah. Some of the terrorist groups, such as Al-Gama'at, have access to credentials for the UN High Commission for Refugees and other UN staff in the former Yugoslavia. Efforts by governments to counter terrorist groups' use of NGOs are complicated by domestic and international political concerns, legal constraints, and the size and flexibility of the international extremist network. Domestic Islamic organisations — and sometimes foreign governments — have accused host governments of attacking legitimate Islamic institutions and intentionally hampering relief efforts. The following 15 organisations employ members or otherwise facilitate the activities of terrorist

- groups operating in Bosnia...and some... not included in this list, have terrorist connections outside of the Balkans: Al- Haramain Islamic Foundation; Human Appeal International Foundation; Human Concern International; Human Relief International; International Humanitarian Relief Organisation (Hilfsorganisation); International Islamic Relief Organisation; Islamic Relief Agency; Kuwait Joint Relief Committee; Islamic Charity Committee; (Probably a subsidiary of the Saudi-based Muslim World League); Human Services Organisation; Muwafaq Foundation; Qatar Charitable Society/Committee; Red Crescent Iran; The Saudi High Commission (Zagreb, Sarajevo, and Tuzla. Operates in Zenica, Mostar, and Split); The Third World Relief Agency and the Islamic World Committee.
22. BrainyQuote.com. "Ovid." Xplore Inc. 2013. [online] Available at: <<http://www.brainyquote.com/quotes/quotes/o/ovid400818.html>> [Accessed 15 July 2013]
23. The Wolfsberg Group. 2011. Wolfsberg Anti-Corruption Guidance. [online] Available at: <<http://www.wolfsberg-principles.com/pdf/Wolfsberg%20Anti%20Corruption%20Guidance%20Paper%20August%202011%20%28Published%29.pdf>> [Accessed 15 July 2013]
24. Organisation for Economic Co-Operation (OECD). 2009. 'Typologies on the Role of Intermediaries in International Business Transactions' [pdf] [online] Available at: <<http://www.oecd.org/investment/anti-bribery/anti-briberyconvention/43879503.pdf>> [Accessed 15 July 2013]
25. Encyclopaedia Britannica. 2013. 'John Emerich Edward Dalberg Acton, 1st Baron Acton' [online] Available at: <<http://www.britannica.com/EBchecked/topic/4647/John-Emerich-Edward-Dalberg-Acton-1st-Baron-Acton/4647suppinfo/Supplemental-Information>> [Accessed 15 July 2013]
26. The Wolfsberg Group. 2013. 'Wolfsberg FAQ's on Politically Exposed Persons' [online] Available at: <<http://www.wolfsberg-principles.com/faq-persons.html>> [Accessed 15 July 2013]
27. Transparency International 2004: Global Corruption Report 2004 [online] Available at: <http://www.files.transparency.org/content/download/479/1974/file/2004_GCR_PoliticalCorruption_EN.pdf> [Accessed 8 September 2013]
28. Bitcoin is 5 years old and has become the flagship of digital currencies, coming of age over the last 12 months, achieving unprecedented attention and increasing legitimacy, but at the same time, still some concern being raised. The popularity of this virtual currency has prompted frantic speculation, as its value has increased from USD 13 at the start of 2013, to a high of over USD 1'200 in November 2013. The future of Bitcoin, as well as other digital currencies which are attempting to gain traction (including ripple, litecoin and others) is likely to depend very much on actions taken in 2014, with many State actors considering how to regulate these new digital currencies. Concerns around the level of anonymity do exist as well as the ability to monitor activity in the currency. Bitcoin is different things to different people: for the purists, it is a functional, free market addendum to an increasingly virtual lifestyle; for others it is merely the opportunity to get rich quick on a currency unassociated with governments and completely unregulated; for others, the ability to conduct almost completely anonymous financial transactions allows a liberation - to launder money and conduct illicit transactions, such as for drugs, weapons or pornography and online sexual services; or as a recent FAQ on the Bitcoin summarized it: "a gigantic goddam mess of idiocy, greed and bad decisions." However, Bitcoin need not be just an instrument for illicit behavior. Bitcoin is often seen to hold greatest value for those developing countries where currency and capital controls are censorious. Some of the more idealistic of supporters also hope that the digital economy can bring social inclusion to those without access to the mainstream financial sector. There are a number of main ways to get Bitcoin: i) there are Exchanges, where you can buy and sell Bitcoin for normal currencies such as in USD and Euros; ii) or you can mine your own via running a computer programme to produce your own, (though this is for most people unlikely as too demanding an exercise demanding significant computing power). Once you have Bitcoins and a Bitcoins wallet (which you can keep online or on your device) you can buy and sell and trade Bitcoins with other Bitcoins users, you can also sell your services to acquire Bitcoins; Copperlark (CLR) - Copperlark is different from other virtual currencies as it uses a completely new algorithm (Keccak, SHA3). It offers faster block times than Bitcoin (4 minutes) and the difficulty re-targets much faster (every 24 hours). CLR can only be mined with a CPU or a GPU through the client. Mining ASICs which are made for SHA256 will not work due to the usage of a new algorithm. There has been a pre-mine of 2 million coins, the developers state that this was to give CLR physical value at the very beginning. Half of the pre-mined coins will be used to promote the currency through banners, articles and ads, the other half will be used for venture investors; Feathercoin (FTC) - Feathercoin is based on Bitcoin's open source software. One of Feathercoins's advantages is that it uses the Scrypt hashing algorithm. This is different from Bitcoin which uses a SHA-256 based hashing algorithm. Scrypt is currently the only viable solution for GPU miners as Bitcoin mining is now dominated by professional ASIC mining hardware. ASICs are expensive but outperforms GPU mining by far. Thus the Scrypt based FTC is safe guarded from the effects of the current available ASIC mining hardware. One of the other big differences over most virtual currencies is the support for Advanced checkpointing. Advanced Check-

pointing allows FTC to send out checkpoints without having to redistribute the Feathercoin software. This works by having a 'master node' which checkpoints each block it sees on the network protecting it from the attacker. This checkpoint is then picked up by all the other clients on the network which will then ignore any blocks generated by a 51% attack. This protects merchants from transaction reversal and miners from losing their newly minted coins. With Advanced Checkpointing, FTC is one of the most secure of all the Scrypt cryptographic currencies; Litecoin (LTC) - Litecoin is the result of some of the Bitcoin community who joined together on IRC in an effort to create a real alternative currency similar to Bitcoin. They wanted to make a virtual currency that is considered silver to Bitcoin's gold. Litecoin aimed to maintain the unique traits and attributes of Bitcoin, while adding to the mixture GPU-resistant mining and a 2.5 minute block rate. This meant that Litecoin wouldn't have a reason to compete with Bitcoin for the used up computational cycles of a graphics card, but working independently on your processor instead. Litecoin uses a memory hard hashing algorithm called scrypt. The algorithm utilises SHA256 and a stream function called salsa20 to force devices that mine it to use a lot of memory or dramatically more ALU cycles to perform a hash. Litecoin was stated to be GPU resistant and started out to be a CPU only coin. However, in late 2011 a solidcoin programmer made the reaper miner which was capable of mining using the GPU at good hashrates. The performance gain was not as big as with Bitcoin but a decent GPU can mine at least 5-10 times faster than a CPU. Since then more and more GPU miners started to move to Litecoin, the coin is still pretty small with low and volatile exchange rates but has a good chance to grow. Litecoin is now a good alternative to Bitcoin where the FPGAs and ASICs are moving in raising the network difficulty so much that mining Bitcoin with a GPU is becoming less profitable; Megacoin (MEC) - Megacoin is a new type of decentralized currency. Not minted or endorsed by any nation, but by users across the globe. Anywhere there is internet, you can send or receive MEC. Even in outer space. There are very little rules for Megacoin. To prevent inflation only a limited supply of 42 million MEC will ever exist. MEC's are mined by users at a set rate for decades into the future. You can get MEC for free by mining or trading for them on an exchange; Mincoin (MNC) - Mincoin is a peer-to-peer virtual currency using the scrypt as a proof-of-work algorithm. MNC has a block target of 1 minute which means it is 10 times faster than Bitcoin and 2.5 times faster than Litecoin. There will only be 2 million coins generated in total which is generally lower than other virtual currencies. MNC was introduced to being Bronze where Bitcoin is Gold. Compared to Litecoin this cryptocurrency does not add any other special features other than a 1 minute block target where Litecoin has a block target of 2.5 minutes; Namecoin (NMC)

- Namecoin is an alternative distributed Domain Name System (DNS) on the basis of Bitcoin software. It expands the software so that transactions for registering, updating, and transferring domains to serve. Like Bitcoin, Namecoin is a peer-to-peer system, which, assuming an honest majority of participants can not be controlled by a single state or a company. Changes to the namespace of the rightful owner of a domain with a public key signature method and distributed to all peer-to-peer users. The inclusion in the block chain-, as the eternal logfile is used, the transactions are authentic. The block chain grows whenever new transactions, if any of the participants through a fairly intense proof-of-work process, a matching result of a cryptographic hash function has found what may be verified by all other participants. The falsification of a longer chain block is, due to the computational effort, impractical. Currently, the top-level domain-bit used in the official domain name system is not awarded. To resolve domain name either the current block chain or use a public name server that participates in the Namecoin system is required. Namecoin uses a separate block of Bitcoin chain. The software is open source and is hosted on GitHub; Novacoin (NVC) - Novacoin is a virtual currency, just like LTC it uses scrypt hashing and thus it can be mined in the same way as Litecoin by CPU and GPU. It has been created by Bitcointalk user Balthazar. Currently it is performing pretty well, selling for higher prices than LTC with lower difficulty on the network; PPCoin (PPCoin) - PPCoin is a virtual currency which has forked from Bitcoin. PPCoin aims to achieve high energy-efficiency while keeping as much as the official Bitcoin properties as possible. PPCoin works with Stake/Proof-of-Stake, this is a term referring to the use of the currency itself to achieve certain goals. PPCoin uses proof-of-stake to provide minting and transaction processing of place of proof-of-work. Unlike Bitcoin ppcoin does not require the use of energy to sustain the network. Proof-of-work currently remains the most practical way of providing initial minting of a virtual currency so it was decided to keep it as part of the hybrid design. Until v0.2, central checkpointing was a critical part of the protocol. The main purpose of this is to defend the network during the growth period and to ensure a smooth upgrade path if any critical vulnerabilities are found. Central checkpointing will slowly be weakened and should eventually be removed from the coin. Unlike Bitcoin there is no hard cap on the amount of coins that will be created. Bitcoin is limited to 21 million coins where PPCoin only has a hard cap of 2 billion coin in the code. There is no intention to limit the amount of coins that can be generated; Phenixcoin (PXC) - Phenixcoin was developed as an internal testing coin for use with various sites. It is based on Litecoin using scrypt as a proof of work scheme. The coin is currently used at a coin based poker site PhenixPoker.com. There are several projects currently

under development which are planned to use the Phenixcoin as their main currency. Because there is already ways to spend Phenixcoin it has more potential then some other virtual currencies; Primecoin (XPM) - Primecoin is the first virtual currency on the market with non-hashcash proof-of-work, generating additional potential scientific value from the mining work. This research is meant to pave the way for other proof-of-work types with diverse scientific computing values to emerge. Several new virtual currencies have been released adopting other hash functions or composition of hash functions for hashcash proof-of-work. It appears there are market forces at play such that diversification of proof-of-work types is inevitable. It could prove difficult for any single type of proof-of-work to maintain dominance in the long term; Protoshares (PTS) - Protoshares uses a new Momentum Proof of Work (POW) algorithm that is designed to be GPU and ASIC resistant. To back this up there is currently a US\$5000 reward for anyone who can prove it is vulnerable to GPUs or ASICs. As well as being an altcoin, Protoshares is a way to own BitShares before they are launched. When BitShares are launched, the genesis block will award one BitShare for every Protoshare held; Quarkcoin (QRK) - Quarkcoin is currently one of the most secure coins as it uses multiple hashing functions. It uses 9 rounds of hashing from 6 hashing functions. 3 rounds will apply a random hashing function. Due to the block reward halving every 3 weeks most coins have been mined already by the early adopters making mining useless at the current price; Terracoin (TRC) - Just like Bitcoin, Terracoin is a peer-to-peer decentralized virtual currency. It has no central issuer but is regulated by a peer-to-peer network instead. Balances, transactions and issuance are all regulated by the network. Other then Bitcoin, Terracoin is going to have a maximum of 42 million coins offering 20 coins per block. This block reward will automatically be halved every 1050000 blocks (4 years). Block generation is also faster then with Bitcoin, the blocks are created every 2 minutes instead of 10 minutes. The first Terracoin blockchain was created on October 26th 2012 making the block reward going down at October 26th 2016 to 10 coins per block; Worldcoin (WDC) - Worldcoin was designed to be the currency of the future. It is very fast but also very secure for day to day transactions. The major goal of worldcoin is to become the virtual currency of choice for merchants and consumer for their everyday transactions, whether it is to buy a cup of coffee or a bigger item. The coin is also apparently based on sound money principals which is supposed to make it the smart choice for wealth preservation. It is designed to appreciate in value over time, unlike paper currencies, this is due to the fact that only 265 million coins will ever be produced.

29. Dinar, A. B. 1998. 'Angola: Diamond Trade and War, 15 Dec 1998' University of Pennsylvania: African Studies Centre [online] Available at: <http://www.africa.upenn.edu/Urgent_Action/apic_121598.html> [Accessed 15 July 2013]

30. Claims that Congolese diamonds are sought and bought by terrorist groups are difficult to prove, but according to Greg Campbell, "Radical Islamic groups funnel millions of dollars made from Congolese diamond sales to their organisations back home [...] members of Hezbollah and other terrorist groups buy diamonds from Congolese miners and middlemen at low cost and smuggle them out of the country." - tbc

31. Global Witness. 2010. 'Conflict diamond scheme must resolve Zimbabwe impasse' [online] Available at: <<http://www.globalwitness.org/library/conflict-diamond-scheme-must-resolve-zimbabwe-impasse>> [Accessed 15 July 2013]

32. The Kimberley Process called for an international certification system on the export and import of diamonds, legislation in all countries to accept only officially sealed packages of diamonds, for countries to impose criminal charges on anyone trafficking in conflict diamonds, and instituted a ban on any individual found trading in conflict diamonds from the diamond bourses of the World Federation of Diamond Bourses. The Kimberley Process was led by the diamond-producing African countries themselves. Also in tourist states like Dubai, before gemstone could be allowed through their airport to other countries, the Kimberley Certification must be presented by the gem's owner. Whilst the KCPS initiative has undoubtedly made life harder for criminals, it has nevertheless failed to stem the flow of blood diamonds, leading key proponents such as Global Witness to publicly abandon the scheme, as they believe that there is no guarantee that diamonds with a Kimberley Process Certification are in fact conflict free, due in large part to corrupt government officials in the leading diamond producing countries, who are prepared to certify that blood diamonds are Kimberley Process Certified. Global Witness stated in 2011 that, "The Kimberley Process's refusal to evolve and address the clear links between diamonds, violence and tyranny has rendered it increasingly outdated, said the group. Despite intensive efforts over many years by a coalition of NGOs, the scheme's main flaws and loopholes have not been fixed and most of the governments that run the scheme continue to show no interest in reform," and "the scheme has failed three tests: it failed to deal with the trade in conflict diamonds from Côte d'Ivoire, was unwilling to take serious action in the face of blatant breaches of the rules over a number of years by Venezuela and has proved unwilling to stop diamonds fuelling corruption and violence in Zimbabwe. It has become an accomplice to diamond laundering, whereby dirty diamonds are mixed in with clean gems." Global Witness. 2011. 'Global Witness leaves Kimberley Process, calls for diamond trade to be held accountable' [online]

- Available at: <<http://www.globalwitness.org/library/global-witness-leaves-kimberley-process-calls-diamond-trade-beheld-accountable>> [Accessed 15 July 2013]
33. Singer, P. W. 2005. 'Outsourcing War' Brookings University Research: Foreign Affairs [online] Available at: <<http://www.brookings.edu/research/articles/2005/03/01usdepartmentofdefense-singer>> [Accessed 15 July 2013]
34. Norton-Taylor, R. 2006. 'Fears over huge growth in Iraq's unregulated private armies' The Guardian Online, 31 Oct 2006. [online] Available at: <<http://www.guardian.co.uk/world/2006/oct/31/iraq.iraqtimeline>> [Accessed 15 July 2013]
35. Singer, P. W. 2003. Corporate Warriors: The Rise of the Privatized Military Industry. Cornell University Press.
36. Financial Action Task Force (FATF). 2007. 'Money Laundering and Terrorist Financing through the Real Estate Sector' [pdf] [online] Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20through%20the%20Real%20Estate%20Sector.pdf>> [Accessed 15 July 2013]
37. Financial Action Task Force (FATF). 2008. 'RBA Guidance for Real Estate Agents' [pdf] [online] Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Guidance%20for%20Real%20Estate%20Agents.pdf>> [Accessed 15 July 2013]

Part 1, Section 2, Sub-section 3 - Products & Services Risks

1. Relbanks.com. 2013 'World's Top Banks' [online] Available at: <<http://www.relbanks.com/worlds-top-banks>> [Accessed 15 July 2013]
2. Towers Watson. 2012. 'The World's 500 largest asset managers – Year end 2011.' [online] Available at: <<http://www.towerswatson.com/en/Insights/IC-Types/Survey-Research-Results/2012/10/the-worlds-500-largest-asset-managers-year-end-2011>> [Accessed 15 July 2013]
3. Investopedia. 2013. 'Definition of Security' [online] Available at: <www.investopedia.com/terms/s/security.asp#axzz2Er1CQlR> [Accessed 15 July 2013]
4. Financial Action Task Force (FATF). 2009. 'Money Laundering and Terrorist Financing in the Securities Sector' [pdf] [online] Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf>> [Accessed 15 July 2013]
5. Bagehot, W. 2004. Lombard Street: A Description of the Money Market. Kessinger Publishing.
6. Gurley, J. G. and Shaw, E. S. 1960. Money in Theory of Finance. Brookings Institution.
7. Financial Action Task Force (FATF). 2008. 'Best Practices Paper: Best Practices on Trade Based Money Laundering' [pdf] [online] Available at: <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf>> [Accessed 15 July 2013]
8. Minority Staff of the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs US Senate. 2001. 'Correspondent Banking: A Gateway for Money Laundering' [pdf] [online] Available at: <<http://www.imolin.org/pdf/imolin/CPRT-107SPRT69919.pdf>> [Accessed 15 July 2013]
9. For details see Part 2, Section 3, Money Laundering Laws and Regulations; FATF
10. A Shell Bank means a bank that (1) does not conduct business at a fixed address in which it is authorized to conduct banking activities, (2) does not employ anybody on a full time basis at that fixed address, (3) does not maintain operating records at that address, (4) is not subject to inspection by the banking authority that licensed it to conduct banking activities. A post office box or electronic address is not a "fixed address" for these purposes.
11. Financial Crimes Enforcement Network, US Department of the Treasury. 2013. 'USA Patriot Act' [online] Available at: <http://www.fincen.gov/statutes_regs/patriot/> [Accessed 15 July 2013]
12. The Wolfsberg Group. 2013. 'Wolfsberg AML Principles for Correspondent Banking' [online] Available at: <<http://www.wolfsberg-principles.com/corresp-banking.html>> [Accessed 15 July 2013]
13. Society for Worldwide Interbank Financial Communications (SWIFT). 2013. 'SWIFT: The global provider of secure financial messaging services' [online] Available at: <<http://www.swift.com/index.page?lang=en>> [Accessed 15 July 2013]
14. SearchQuotes.com. 2013. 'Andrew Tobias Quotes' [online] Available at: <http://www.searchquotes.com/quotation/You_want_21_percent_risk_free%3F_Pay_off_your_credit_cards./194768/> [Accessed 16 July 2013]
15. Creditcards.com. 2013. 'Credit card statistics, industry facts, debt statistics' [online] Available at: <<http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php>> [Accessed 16 July 2013]
16. The Nilson Report. 2013. 'Charts and Graphs Archive' [online] Available at: <http://www.nilsonreport.com/publication_chart_and_graphs_archive.php?1=1&year=2013> [Accessed 16 July 2013]
17. Statistic Brain. 2012. 'Credit Card Fraud Statistics' [online] Available at: <<http://statisticbrain.com/credit-card-fraud-statistics>> [Accessed 16 July 2013]

18. The Wolfsberg Group. 2013. 'Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities' [online] Available at: <<http://www.wolfsberg-principles.com/credit-merchant.html>> [Accessed 16 July 2013]
19. The Wolfsberg Group. 2011. 'Wolfsberg Guidance on Prepaid and Stored Value Cards' [pdf] [online] Available at: <http://www.wolfsberg-principles.com/pdf/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf> [Accessed 15 July 2013]
20. 4. Niall Ferguson. 2010. 'The People's Banker' 10 Aug 2010. [online] Available at: <<http://www.niallferguson.com/journalism/finance-economics/the-peoples-banker>> [Accessed 16 July 2013]
21. Bulge Bracket as a phrase came from the way investment banks are listed on the "tombstone", or public notification of a financial transaction or deal. The bank responsible for control of allocation of securities to investors, known as the book running manager is listed above the others and on the cover of the prospectus. The font size of the name of this bank, or banks if there are co-book running managers, is larger and it may "bulge" out. There is often debate over which banks are considered to belong to the bulge bracket. Membership implies prestige but there are no precise criteria for inclusion, and financial power is transient. Various rankings are often cited, such as Thomson Reuters League Tables, Bloomberg 20, or other league tables. In the late 1960s and early 1970s, the top tier of Investment Banks called the bulge bracket, consisted of Morgan Stanley; First Boston; Kuhn, Loeb; and Dillon, Read." By the middle of the 1970s, Kuhn, Loeb; and Dillon, Read would be replaced with Salomon Brothers, Goldman Sachs, and Merrill Lynch. Just prior to the Global Financial crisis in 2007, the Bulge Bracket firms were, alphabetically: Bear Stearns, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, JP Morgan Chase, Lehman Brothers, Merrill Lynch, Morgan Stanley, and UBS. This list has changed as a result of the 2008 subprime mortgage crisis, with Lehman Brothers having filed for bankruptcy (later having their core US investment bank acquired by Barclays), Bear Stearns collapsing and being sold to JP Morgan Chase at \$2 per share and Merrill Lynch being purchased by Bank of America. Bank of America Merrill Lynch gained Bulge Bracket status after its acquisition. The following acquisitions led to the demise and rise of the current crop of Bulge Bracket firms: S.G Warburg & Co and then Dillon, Read & Co., acquired by Swiss Bank Corporation (eventually UBS) in 1995 & 1997 respectively. First Boston, acquired by Credit Suisse in 1988 and branded Credit Suisse First Boston, later renamed to Credit Suisse. Kuhn, Loeb & Co., merged with Lehman Brothers in 1977, forming Lehman Brothers, Kuhn, Loeb Inc. Lehman Brothers, declared bankrupt in September 2008. The Asian and European operations were bought by Nomura. Barclays acquired the North American Lehman operations. Merrill Lynch, acquired by Bank of America in September 2008. UK's Morgan, Grenfell & Co., acquired by Deutsche Bank in 1990, and Bankers Trust in 1998. Salomon Brothers, acquired by Travellers Group (eventually Citigroup) in 1998
22. Investopedia. 2012. 'Are Derivatives a Disaster Waiting to Happen?' 26 Oct 2012 [online] Available at: <<http://www.investopedia.com/articles/optioninvestor/08/derivative-risks.asp>> [Accessed 16 July 2013]
23. Key Private Bank. 2013. 'Insights: Deriving Value from Derivatives' [pdf] [online] Available at: <<https://www.key.com/kco/images/nws-private-banking-derivatives-white.pdf>> [Accessed 16 July 2013]
24. Berkshire Hathaway Inc. 2003. 'Letters to 2002' [pdf] [online] Available at: <<http://berkshirehathaway.com/letters/2002pdf.pdf>> [Accessed 16 July 2013]
25. Warren Buffett writing about his 1998 acquisition of General Reinsurance Corp (pp7/8) <http://www.berkshire-hathaway.com/letters/2002pdf.pdf> [accessed 21/05/13] - Buffett's perspective may well have been driven by his own experience with some derivative positions he inherited as a result of Berkshire's \$22 billion purchase of General Reinsurance Corporation in 1998 (the largest US property and casualty reinsurer at the time). General Reinsurance Securities, a subsidiary of General Reinsurance initiated in 1990, was a derivatives dealer tied to global financial markets. Unfortunately, this relationship had unpredictable consequences. Buffett wanted to sell the subsidiary, but he could not find an agreeable counterparty (buyer). So, he decided to close it, which was easier said than done, as this decision required him to unwind the subsidiary's derivative positions. He likens this unwinding task to entering hell, stating that derivatives positions were "easy to enter and almost impossible to exit." As a result, General Reinsurance recorded a \$173 million pre tax loss in 2002.
26. Chinese Walls are an ethical barrier between different divisions of a financial institution to avoid conflicts of interest such as between corporate advisory activity on the one hand and trading / brokering on the other. This separates those giving corporate advice on takeovers from those advising clients about buying shares. The "wall" is established to prevent leaks of material non-public information which could influence the advice given to clients making investments and allow staff to take advantage of facts that are not yet known to the general public...see also (a) <http://www.investopedia.com/terms/c/chinesewall.asp> <http://fshandbook.info/FS/html/handbook/SYSC/10/2> [21/05/13] and Financial Conduct Authority, Bank of England. 2013. 'Senior Management Arrangements, Systems and Controls: Chapter 10: Conflicts of Interest' [pdf] [online] Available at: <<http://media.fshandbook.info/content/>

- full/SYSC/10/2.pdf> [Accessed 16 July 2013]
27. The Quotations Page. 2013. 'Quote Details: Bob Hope' [online] Available at: <<http://www.quotationspage.com/quote/99.html>> [Accessed 15 July 2013]
28. <http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTRESEARCH/0,,contentMDK:20652043-pagePK:64214825-piPK:64214943-theSitePK:469382,00.html>
29. Financial Action Task Force (FATF). 2013. 'What money laundering?' [online] Available at: <<http://www.fatf-gafi.org/pages/faq/moneylaundering/>> [Accessed 16 July 2013]
30. The UN Office on Drugs and Crime (UNODC) issued a report on 25 October 2011 entitled "Estimating illicit financial flows resulting from drug trafficking and other transnational organised crime," which estimated that criminal proceeds, excluding tax evasion, would amount to some \$2.1 trillion or 3.6% of GDP in 2009, with US\$1.6 trillion being laundered. Of this total, the proceeds of transnational organised crime, such as drug trafficking, counterfeiting, human trafficking and small arms smuggling, would amount to 1.5% of 2009 global GDP, 70% of which or would likely have been laundered through the financial system. The Report stated that only 0.2% of illicit financial flows are currently being seized and frozen. UNODC [online]. 2011. Available from: <http://www.unodc.org/documents/data-and-analysis/Studies/Illlicit_financial_flows_2011_web.pdf> [Accessed 14 July 2013]
31. Wikipedia. 2013. 'Automated Teller Machine' 20 June 2013 [online] Available at: <http://en.wikipedia.org/wiki/Automated_teller_machine> [Accessed 16 July 2013]
32. US Government Printing Office. 2000. 'Private Banking and Money Laundering: A case study of opportunities and vulnerabilities' [online] Available at: <<http://goo.gl/7rFVm>> [Accessed 16 July 2013]
33. Becerra, J., Damisch, P., Holley, B., Jumar, M., Naumann, M., Tang, T., Zakrzewski, A. 2010. 'The Offshore Business Has Recovered – but Challenges Remain' Global Wealth, June 10 2010. [online] Available at: <http://www.bcgperspectives.com/content/articles/offshore_business_recovered_challenges_remain/> [Accessed 16 July 2013]
34. Merrill Lynch Wealth Management. 2011. 'World Wealth Report' [pdf] [online] Available at: <<http://www.ml.com/media/114235.pdf>> [Accessed 16 July 2013]
35. Scorpio Partnership. 2012. [press release] 'Wealth Management Partnership Private Banking Benchmark 2012' [online] Available at: <http://www.scorpiopartnership.com/uploads/pdfs/120718_ScorpioPartnership_Private%20Banking%20Benchmark_FINAL.pdf> [Accessed 16 July 2013]
36. Financial Crimes Enforcement Network, US Department of the Treasury. 2013. 'USA Patriot Act' [online] Available at: <http://www.fincen.gov/statutes_regs/patriot/> [Accessed 15 July 2013]
37. Banks' management of high money laundering risk situations issued by UK's FSA in June 2011: [online] Available at <http://www.fsa.gov.uk/pubs/other/aml_final_report.pdf> [Accessed 18 August 2013]
38. Joint Money Laundering Steering Group (JMLSG). 2013. 'Other helpful material' [online] Available at: <<http://www.jmlsg.org.uk/industry-guidance/article/guidance>> [Accessed 16 July 2013]

Part 1, Section 2, Sub-section 4, Country Risks

Country Risks Methodology and Sources

1. Financial Actions Task Force (FATF). 2013. 'FATF Public Statement 2013' [online] Available at: <<http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatfpublicstatement22february2013.html>> [Accessed 16 July 2013]
2. UN. 2013. 'Charter of the UN: Chapter VII: Action with respect to threats to the peace, breaches of the peace, and acts of aggression' [online] Available at: <<http://www.un.org/en/documents/charter/chapter7.shtml>> [Accessed 15 July 2013]
3. European Union. 2010. 'Information and Notices' Official Journal of the European Union, Vol 53. [pdf] [online] Available at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:326:FULL:EN:PDF>> [Accessed 16 July 2013]
4. European Union External Action. 2013. 'Sanctions or Restrictive Measures' [online] Available at: <http://eeas.europa.eu/cfsp/sanctions/index_en.htm> [Accessed 16 July 2013]
5. State Secretariat for Economic Affairs (SECO). 2013. 'Sanctions/Embargoes' [online] Available at: <<http://www.seco.admin.ch/themen/00513/00620/index.html?lang=en>> [Accessed 16 July 2013]
6. The Wolfsberg Group. 2013. 'Wolfsberg Statement – Guidance on a Risk Based Approach for Managing Money Laundering Risks' [online] Available at: <<http://www.wolfsberg-principles.com/risk-based-approach.html>> [Accessed 15 July 2013]
7. International Centre for Asset Recovery. 2013. 'Welcome to the Basel AML Index 2013' [online] Available at: <<http://index.baselgovernance.org/>> [Accessed 16 July 2013]

8. Bertelsmann Stiftung. 2013. 'Transformation Index BTI' [online] Available at: <http://www.bertelsmann-stiftung.de/cps/rde/xchg/SID-7416E337-45920379/bst_engl/hs.xsl/307.htm> [Accessed 16 July 2013]
9. Control Risks. 2013. 'Homepage' [online] Available at: <<http://www.controlisks.com/pages/home.aspx>> [Accessed 16 July 2013]
10. The Egmont Group of Financial Intelligence Units. 2013. 'Homepage' [online] Available at: <<http://www.egmontgroup.org/>> [Accessed 16 July 2013]
11. Mortimer, A. 2012. 'ECR: Country Risk Q1 2012 results – Eurozone stabilizes in global rankings' Euromoney, 3 April 2012. [online] Available at: <<http://www.euromoney.com/article/3006360/ECR-Country-Risk-Q1-2012-resultsEurozone-stabilizes-in-global-rankings.html>> [Accessed 16 July 2013]
12. EU 2012. 'Common understanding between EU Member States on the procedure and criteria for the recognition of third countries equivalence under directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing' [pdf] [online] Available at: <http://ec.europa.eu/internal_market/company/docs/financial-crime/3rd-country-common-understanding_en.pdfs> [Accessed 16 July 2013]
13. Freedom House. 2013. 'Freedom in the World 2013' [online] Available at: <<http://www.freedomhouse.org/report/freedom-world/freedom-world-2013>> [Accessed 16 July 2013]
14. Organisation for Economic Co-operation (OECD). 2013. 'Global Forum on Transparency and Exchange of Information for Tax Purposes' [online] Available at: <<http://www.oecd.org/tax/transparency/>> [Accessed 16 July 2013]
15. Transparency International. 2013. 'Corruption Perceptions Index' [online] Available at: <<http://www.transparency.org/research/cpi/overview>> [Accessed 16 July 2013]
16. Transparency International. 2013. 'Global Corruption Barometer' [online] Available at: <<http://www.transparency.org/research/gcb/overview>> [Accessed 16 July 2013]
17. U.S. Department of State. 2013. 'Country Reports on Terrorism 2011' [online] Available at: <<http://www.state.gov/jl/ct/rls/crt/2011/index.htm>> [Accessed 16 July 2013]
18. U.S. Department of State. 2013. '2013 International Narcotics Control Strategy Report' [online] Available at: <<http://www.state.gov/jnl/rls/nrcpt/2013/>> [Accessed 16 July 2013]
19. U.S. Department of State. 2013. 'Trafficking in Persons Report 2010' [online] Available at: <<http://www.state.gov/j/tip/rls/tiprpt/2010/>> [Accessed 16 July 2013]
20. Fund For Peace. 2012. 'The Failed States Index 2012' [online] Available at: <<http://ffp.statesindex.org/rankings-2012-sortable>> [Accessed 16 July 2013]
21. The World Bank Worldwide Governance Indicators: [online] Available at: <http://www.info.worldbank.org/governance/wgi/sc_country.asp> [Accessed 6 September 2013]
22. The World Bank. 2013. 'Ease of doing business index (1=most business-friendly regulations)' [online] Available at: <<http://data.worldbank.org/indicator/IC.BUS.EASE.XQ>> [Accessed 16 July 2013]
23. KnowYourCountry.com. 2013. 'KnowYourCountry' 15 July 2013 [online] Available at: <<http://knowyourcountry.com/>> [Accessed 16 July 2013]

Part 1, Section 3 - Money Laundering Laws & Regulations

Introduction

1. UN Office on Drugs and Crime. 2009. 'This day in history: The Shanghai Opium Commission , 1909' [online] Available at: <<http://www.unodc.org/unodc/en/frontpage/this-day-in-history-the-shanghai-opium-commission-1909.html>> [Accessed 16 July 2013]
2. UN Office on Drugs and Crime. 2009. 'The Hague International Opium Convention' [online] Available at: <<http://www.unodc.org/unodc/en/frontpage/the-1912-hague-international-opium-convention.html>> [Accessed 16 July 2013]

Part 1, Section 3 - AML Treaties, Conventions & Major Laws

1. Article 10 of The International Opium Convention ("The Hague Convention"). (1912) [online] Available at: <http://en.wikisource.org/wiki/International_Opium_Convention#Article_10> [Accessed 18 June 2013]
2. The International Opium Convention ("The Geneva Convention"). (1925) [online] Available at: <http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-6-a&chapter=6&lang=en> [Accessed 18 June 2013]
3. Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare. (1925) [online] Available at: <http://www.un.org/disarmament/WMD/Bio/pdf>Status_Protocol.pdf> [Accessed 18 June 2013]
4. US Securities Act of 1933. (1933) [online] Available at: <<http://www.sec.gov/about/laws/sa33.pdf>> [Accessed 18 June 2013]

5. US Banking Act of 1933 (“Glass-Steagall Act”). (1933) [online] Available at: <http://en.wikisource.org/wiki/Banking_Act_of_1933> [Accessed 18 June 2013]
6. US Securities and Exchange Act. (1934) [online] Available at: <<http://taft.law.uc.edu/CCL/34Act/>> [Accessed 18 June 2013]
7. US Commodity Exchange Act (“Grain Futures Act”). (1936) [online] Available at: <<http://www.law.cornell.edu/uscode/text/7/chapter-1>> [Accessed 18 June 2013]
8. US Exchange Act Rule 10b-5. (1945) [online] Available at: <<http://www.gpo.gov/fdsys/pkg/CFR-2011-title17-vol3/xml/CFR-2011-title17-vol3-sec240-10b-5.xml>> [Accessed 18 June 2013]
9. Single Convention on Narcotic Drugs (amended by the 1972 Protocol amending the Single Convention on Narcotic Drugs, 1961). (1961) [online] Available at: <http://www.unodc.org/pdf/convention_1961_en.pdf> [Accessed 18 June 2013]
10. Convention on Offences and Certain Other Acts Committed on Board Aircraft (“Tokyo Convention”). (1969) [online] Available at: <<http://www.un.org/en/sc/ctc/docs/conventions/Conv1.pdf>> [Accessed 18 June 2013]
11. US Crime Control Act 1970(the “Organised Crime Act”)
12. Racketeer Influenced and Corrupt Organisations Act (“RICO Act”), enacted by section 901(a) of the Organised Crime Control Act. (1970) [online] Available at: <<http://www.law.cornell.edu/uscode/text/18/part-I/chapter-96>> [Accessed 18 June 2013]
13. Treaty on the Non-Proliferation of Nuclear Weapons (NPT). (1970) [online] Available at: <<http://www.un.org/disarmament/WMD/Nuclear/NPTtext.shtml>> [Accessed 18 June 2013]
14. Bank Secrecy Act 1970 (“BSA”, “Currency and Foreign Transactions Reporting Act”). (1970) Available at: <http://www.finncen.gov/statutes_regs/bsa/> [Accessed 18 June 2013]
15. Convention for the Suppression of Unlawful Seizure of Aircraft (the “Hague Convention”). (1971) [online] Available at: <<http://www.un.org/en/sc/ctc/docs/conventions/Conv2.pdf>> [Accessed 18 June 2013]
16. Convention for the suppression of unlawful acts against the safety of civil aviation (“Montreal Convention”). (1971) [online] Available at: <<http://treaties.un.org/untc//Pages//doc/Publication/UNTS/Volume%20974/volume-974-I-14118-English.pdf>> [Accessed 18 June 2013]
17. Convention on Psychotropic Substances. (1971) [online] Available at: <http://www.unodc.org/pdf/convention_1971_en.pdf> [Accessed 18 June 2013]
18. The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons (“Biological Weapons Convention (BWC)”). (1972) [online] Available at: <[http://www.unog.ch/80256EE600585943/\(httpPages\)/04FBDD6315AC720C1257180004B1B2F?OpenDocument](http://www.unog.ch/80256EE600585943/(httpPages)/04FBDD6315AC720C1257180004B1B2F?OpenDocument)> [Accessed 18 June 2013]
19. Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents. (1973) [online] Available at: <http://untreaty.un.org/ilc/texts/instruments/english/conventions/9_4_1973.pdf> [Accessed 18 June 2013]
20. Convention on International Trade in Endangered Species of Wild Flora and Fauna (“CITES” or the “Washington Convention”). (1975) [online] Available at: <<http://www.cites.org/eng/disc/E-SV-indicators.pdf>> [Accessed 18 June 2013]
21. The Agreement on the Swiss Banks’ Code of Conduct with Regard to the Exercise of Due Diligence (CDB). (1977, revised latest 2008) [online] Available at: <<http://www.swissbanking.org/en/20080410-vsbl-cwe.pdf>> [Accessed 18 June 2013]
22. The Foreign Corrupt Practices Act (FCPA). (1977) [online] Available at: <<http://www.justice.gov/criminal/fraud/fcpa/docs/fcpa-english.pdf>> [Accessed 18 June 2013]
23. International Convention against the Taking of Hostages (The “Hostage Convention”). (1983) [online] Available at: <<http://www.un.org/en/sc/ctc/docs/conventions/Conv5.pdf>> [Accessed 18 June 2013]
24. US Insider Trading Sanctions Act. (1984) [online] Available at:
25. UK Company Securities (Insider Dealing) Act. (1985) [online] Available at: <http://www.legislation.gov.uk/ukpga/1985/8/pdfs/ukpga_19850008_en.pdf> [Accessed 18 June 2013]
26. US Money Laundering Control Act. (1986) [online] Available at: <http://www.ffiec.gov/bsa_amf_infobase/documents/regulations/ML_Control_1986.pdf> [Accessed 18 June 2013]
27. Convention on the Physical Protection of Nuclear Material (CPPNM). (1987) [online] Available at <<http://www.un.org/en/sc/ctc/docs/conventions/Conv6.pdf>> [Accessed 18 June 2013]
28. Convention for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation. (1988) [online] Available at: <<http://www.un.org/en/sc/ctc/docs/conventions/Conv7.pdf>> [Accessed 18 June 2013]
29. Basel Committee on Banking Supervision Prevention of Criminal use of the Banking System for the Purpose of Money Laundering. (1988) [online] Available at: <<http://www.bis.org/publ/bcbcl37.pdf>> [Accessed 18 June 2013]
30. UN Convention Against Illicit Traffick in Narcotic Drugs and Psychotropic Substances (the “Vienna Convention”). (1988) [online] Available at: <http://www.unodc.org/pdf/convention_1988_en.pdf> [Accessed 18 June 2013]
31. European Community Directive Coordinating Regulations on Insider Trading. (1989) [online] Available at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31989L0592:EN:HTML>> [Accessed 18 June 2013]
32. The Forty Recommendations of the Financial Action Task Force on Money Laundering. (1990) [online] Available at: <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf>> [Accessed 18 June 2013]
33. Council Directive on Prevention of the use of the Financial System for the Purpose of Money Laundering. (1991) [online] Available at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0308:EN:H>> [Accessed 18 June 2013]
34. Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation. (1992) [online] Available at: <<http://www.un.org/en/sc/ctc/docs/conventions/Conv8.pdf>> [Accessed 18 June 2013]
35. Convention on Biological Diversity (CDB). (1993) [online] Available at: <<http://www.cbd.int/doc/legal/cbd-en.pdf>> [Accessed 18 June 2013]
36. The Chemical Weapons Convention. (1993) [online] <<http://www.fas.harvard.edu/~hsp/cwc/cwc.html>> [Accessed 18 June 2013]
37. US Inter-American Convention Against Corruption. (1996) [online] Available at: <<http://www.oas.org/juridico/english/treaties/b-58.html>> [Accessed 18 June 2013]
38. The Forty Recommendations of the Financial Action Task Force on Money Laundering (revised). (1996) [online] Available at: <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201996.pdf>> [Accessed 18 June 2013]
39. International Convention for the Suppression of Terrorist Bombings (“Terrorist Bombings Convention”). (1997) [online] Available at: <<http://www.un.org/en/sc/ctc/docs/conventions/Conv11.pdf>> [Accessed 18 June 2013]
40. UN Political Declaration and Action Plan Against Money Laundering. (1998) [online] Available at: <<http://www.imolin.org/imolin/ungadec.html>> [Accessed 18 June 2013]
41. Council of Europe Criminal Law Convention & Civil Law Convention. (1998) [online] Available at: <http://archive.transparency.org/global_priorities/international_conventions/conventions_instruments/coe_crime_laws> [Accessed 18 June 2013]
42. Basel Committee on Banking Supervision. “Prevention of criminal use of the banking system for the purpose of money laundering2. (1998) [online] Available at: <<http://www.bis.org/publ/bcbx137.html>> [Accessed to be xxxx]
43. Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. (1999) [online] Available at: <<http://www.oecd.org/daf/anti-bribery/anti-briberyconvention/38028044.pdf>> [Accessed 18 June 2013]
44. International Convention for the Suppression of the Financing of Terrorism (“The Terrorist Financing Convention”). (1999) [online] Available at: <<http://www.un.org/law/cod/finterr.htm>> [Accessed 18 June 2013]
45. USA Financial Services Modernisation Act (“Gramm-Leach-Bliley Act”). (1999) [online] Available at: <<http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>> [Accessed 18 June 2013]
46. Convention against Transnational Organised Crime (the “Palermo Convention”). (2001) [online] Available at: <<http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>> [Accessed 18 June 2013]
47. Second Directive on Prevention of the use of the Financial System for the Purpose of Money Laundering (Amending Council Directive 91/308/EEC). (2001) [online] Available at: <http://www.esma.europa.eu/system/files/MoneylaunderingDir_2001_97.pdf> [Accessed 18 June 2013]
48. Basel Committee on Banking Supervision: Customer Due Diligence Paper for Banks. (2001) [online] Available at: <<http://www.bis.org/publ/bcbx85.htm>> [Accessed 18 June 2013]
49. Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001 (“PATRIOT”). (2001) [online] Available at: <<http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>> [Accessed 18 June 2013]
50. Financial Action Task Force 8 Special Recommendations on Terrorism Finance (2004, amended to become 9 special recommendations). (2001) [online] Available at: <<http://www.fatf-gafi.org/media/fatf/documents/reports/>>

FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf> [Accessed 18 June 2013]

51. Act to Protect Investors by Improving the Accuracy and Reliability of Corporate Disclosures made Pursuant to the Securities Laws and for Other Purposes (also known as “Public Company Accounting Reform and Investor Protection Act”, “Corporate and Auditing Accountability and Responsibility Act”, “Sarbanes Oxley/SOX”). (2002) [online] Available at: <<http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf>> [Accessed 18 June 2013]

52. Financial Action Task Force 40+8 Recommendations – Revised. (2003) [online] Available at: <<http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf>> [Accessed 18 June 2013]

53. UN Convention against Corruption (UNCAC). (2003) [online] Available at: <http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf> [Accessed 18 June 2013]

54. The Trafficking in Persons Protocol (Palermo Protocol), Protocol to the Convention Against Transnational Organised Crime. (2003) [online] Available at: <<http://www1.umn.edu/humanrts/instree/trafficking.html>> [Accessed 18 June 2013]

55. African Union Convention on Preventing and Combating Corruption. (2003) [online] Available at: <<http://www.africa-union.org/root/au/Documents/Treaties/Text/Convention%20on%20Combating%20Corruption.pdf>> [Accessed 18 June 2013]

56. Basel Committee on Banking Supervision issued a General Guide to Account Opening and Customer Satisfaction. (2003) [online] Available at: <<http://www.bis.org/publ/bcbs85annex.htm>> [Accessed 18 June 2013]

57. The Smuggling of Migrants by Land, Sea and Air – Palermo Protocol (Protocol to the Convention against Transnational Organised Crime 2000). (2004) [online] Available at: <http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_smug_eng.pdf> [Accessed 18 June 2013]

58. Basel Committee on Banking Supervision issued its “Consolidated KYC Risk Management”. (2004) [online] Available at: <<http://www.bis.org/publ/bcbs110.pdf>> [Accessed 18 June 2013]

59. European Union Market Abuse Directive (“MAD”). (2005) [online] Available at: <http://ec.europa.eu/internal_market/finances/docs/actionplan/transposition/uk/d13.2-uk.pdf> [Accessed 18 June 2013]

60. Third Directive on Prevention of the use of the Financial System for the Purpose of Money Laundering. (2005) [online] Available at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:en:PDF>> [Accessed 18 June 2013]

61. Protocol Against the Illicit Manufacturing and Trafficking in Firearms, their Parts and Components and Ammunition – Palermo Protocol (Protocol to the Convention Against Transnational Organised Crime 2000). (2005) [online] Available at: <<http://www.unodc.org/documents/treaties/Special/2001%20Protocol%20against%20the%20Illicit%20Manufacturing%20of%20and%20Trafficking%20in%20Firearms.pdf>> [Accessed 18 June 2013]

62. Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation. (2005) [online] Available at: <<https://www.unodc.org/tldb/pdf/Protocol%20Fixed%20Platforms%20EN.pdf>> [Accessed 18 June 2013]

63. Swiss Financial Market Supervisory Authority (FINMA): Market Conduct Rules. (2008) [online] Available at: <<http://www.finma.ch/e/regulierung/Documents/finma-rs-2008-38-e.pdf>> [Accessed 18 June 2013]

64. Financial Services and Markets Act 2000 (FSMA). (2000) [online] Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/81410/consolidated_fsma050911.pdf> [Accessed 18 June 2013]

65. Financial Services Authority Code of Market Conduct. (2009) [online] Available at: <http://www.legislation.gov.uk/ksi/2009/3128/pdfs/ksi_20093128_en.pdf> [Accessed 18 June 2013]

66. Organisation for Economic Co-operation and Development: Recommendations for Further Combating Bribery of Foreign Public Officials in International Business Transactions. (2009) [online] Available at: <<http://www.oecd.org/investment/anti-bribery/anti-briberyconvention/44176910.pdf>> [Accessed 18 June 2013]

67. The Foreign Account Tax Compliance Act (FATCA). (2010) [online] Available at: <<http://www.gpo.gov/fdsys/pkg/PLAW-111publ147/pdf/PLAW-111publ147.pdf>> [Accessed 18 June 2013]

68. United Kingdom Bribery Act. (2010) [online] Available at: <<http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf>> [Accessed 18 June 2013]

69. Convention on Cluster Munitions (CCM). (2010) [online] Available at: <[http://www.unog.ch/80256EDD006B8954/\(httpAssets\)/CE9E6C29A6941AF1C12574F7004D3A5C/\\$file/ccm77_english.pdf](http://www.unog.ch/80256EDD006B8954/(httpAssets)/CE9E6C29A6941AF1C12574F7004D3A5C/$file/ccm77_english.pdf)> [Accessed 18 June 2013]

70. The Dodd-Frank Wall Street Reform and Consumer Protection Act. (2010) [online] Available at: <<http://www.sec.gov/about/laws/wallstreetreform-cpa.pdf>> [Accessed 18 June 2013]

71. European Union Second Market Abuse Directive (“MAD 2”) – Proposals. (2011) [online] Available at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0654:FIN:EN:PDF>> [Accessed 18 June 2013]
72. The Financial Action Task Force Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. (2012) [online] Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> [Accessed 18 June 2013]
73. Swiss Stock Exchange Act (Amended)
74. European Union Fourth Anti-Money Laundering Directive: Proposed and Funds Transfer Regulations Proposed. (2012) [online] Available at: <<http://www.european-compliance.com/Library/MMs/201305.pdf>> [Accessed 18 June 2013]
75. European Union Directive on Freezing and Confiscation of the Proceeds of Crime – Proposed. (2012) [online] Available at: <http://www.ecba.org/extdocserv/201210_assetseizureECBA_statement.pdf> [Accessed 18 June 2013]
76. Financial Crimes Enforcement Network: Advance Notice of Proposed Rulemaking on Customer Due Diligence – Proposed. (2012) [online] Available at: <http://www.fincen.gov/statutes_regs/frn/pdf/1506-AB15_CDD%20AN-PRM.pdf> [Accessed 18 June 2013]
77. Federal Act on War Materials. (2013) [online] Available at: <<http://www.admin.ch/ch/e/rs/5/514.51.en.pdf>> [Accessed 18 June 2013]
78. Money Laundering Act: Proposed implementation of (a) FATF recommendations and (b) Financial Market Strategy (“Federal Council commences work on implementing FATF recommendations”). (2012) [online] Available at: <http://www.news.admin.ch/message/index.html?lang=en&msg_id=44173> [Accessed 18 June 2013]
79. UN Arms Trade Treaty (ATT). (2013) [online] Available at: <http://treaties.un.org/doc/Treaties/2013/04/20130410%2012-01%20PM/Ch_XXVI_08.pdf#page=21> [Accessed 18 June 2013]
80. Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Singapore). (2013) [online] Available at: <<http://www.imolin.org/doc/amlid2/Sgp%20CD%20Act.pdf>> [Accessed 18 June 2013]
81. Basel Committee on Banking Supervision. “Sound management of risks related to money laundering and financing of terrorism”, consultative document (2013) Available at: <<http://www.bis.org/publ/bcbs252.html>> [Accessed 23 July 2013]

Financial Action Task Force /FATF

1. Methodology for assessing technical compliance with the FATF recommendations and the Effectiveness of AML/CFT systems. <<http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%202022%20Feb%202013.pdf>> [Accessed 14/05/13]
2. Guidance on Anti-Money Laundering and Counter Terrorist Financing Measures and Financial Inclusion. <http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf> [Accessed 14/05/13]
3. FATF International Standards (2012) <<http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html>> [Accessed 14/05/13]
4. Money Laundering and Terrorist Financing vulnerabilities of the illicit tobacco trade. <<http://www.fatf-gafi.org/media/fatf/documents/reports/Illicit%20Tobacco%20Trade.pdf>> [Accessed 24/05/13]
5. Operational Issues – Financial Information Guidance . <http://www.fatf-gafi.org/topics/methodsandtrends/documents/operationalissues-financialinvestigationsguidance.html> Specific Risk Factors in the Laundering of Proceeds of Corruption - assistance to Reporting Institutions <<http://www.fatf-gafi.org/topics/corruption/documents/specifickriskfactorsinthelaunderingofproceeds-of-corruption-assistance-reporting-institutions.html>> [Accessed 24/05/13]
6. G20 Finance Ministers and Central Bank Governors reaffirming commitment to the FATF. <<http://www.fatf-gafi.org/documents/documents/ministersoffinanceandcentralbankgovernorsoftheg20/reaffirmcommitmenttothefatf.html>> [Accessed 24/05/13]
7. Laundering the proceeds of Corruption. <<http://www.fatf-gafi.org/media/fatf/documents/reports/Laundering%20the%20Proceeds%20of%20Corruption.pdf>> [Accessed 24/05/13]
8. Organised Maritime Piracy and Related Kidnapping for ransom. <<http://www.fatf-gafi.org/topics/methodsandtrends/documents/organisedmaritimepiracyandrelatedkidnappingforransom.html>> [Accessed 24/05/13]
9. Money Laundering Risks Arising from Trafficking of Human Beings and Smuggling of Migrants <<http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingrisksarisingfromtraffickingofhumanbeingsandsmugglingofmigrants.html>> [Accessed 24/05/13]
10. Money Laundering Using Trusts and Company Service Providers (TSCP’s) <<http://www.fatf-gafi.org/media/>

[fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers.pdf) [Accessed 24/05/13]
 11. Money Laundering using New Payment Methods. <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>> [Accessed 24/05/13]
 12. Global Money Laundering and Terrorist Financing Threat Assessment. <<http://www.fatf-gafi.org/media/fatf/documents/reports/Global%20Threat%20assessment.pdf>> [Accessed 24/05/13]
 13. Money Laundering through Money Remittance and Currency Exchange providers. <<http://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf>> [Accessed 24/05/13]
 14. Money Laundering vulnerabilities of Free Trade Zones <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf>> [Accessed 24/05/13]
 15. Money Laundering and Terrorism Finance in the Securities Sector. <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf>> [Accessed 24/05/13]
 16. Money Laundering through the Football Sector. <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20through%20the%20Football%20Sector.pdf>> [Accessed 24/05/13]
 17. Vulnerabilities of Casinos and Gaming Sector. <<http://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf>> [Accessed 24/05/13]
 18. Typologies Report on Proliferation Finance <<http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>> [Accessed 24/05/13]
 19. Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems. <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf>> [Accessed 24/05/13]
 20. Money Laundering & Terrorist Financing Risk Assessment Strategies. <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20Risk%20Assessment%20Strategies.pdf>> [Accessed 24/05/13]
 21. Terrorist Financing Typologies Report. <<http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf>> [Accessed 24/05/13]
 22. Money Laundering & Terrorist Financing through the Real Estate Sector. <<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20through%20the%20Real%20Estate%20Sector.pdf>> [Accessed 24/05/13]
 23. Laundering the proceeds of VAT Carousel Fraud. <<http://www.fatf-gafi.org/media/fatf/documents/reports/Laundering%20the%20Proceeds%20of%20VAT%20Carousel%20Fraud.pdf>> [Accessed 24/05/13]
 24. The Misuse of Corporate vehicles , including Trust and Company service providers. <<http://www.fatf-gafi.org/media/fatf/documents/reports/Misuse%20of%20Corporate%20Vehicles%20including%20Trusts%20and%20Company%20Services%20Providers.pdf>> [Accessed 24/05/13]
 25. Report on New Payment Methods <<http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf>> [Accessed 24/05/13]
 26. Trade Based Money Laundering. <<http://www.fatf-gafi.org/topics/methodsandtrends/documents/trade-based-moneylaundering.html>> [Accessed 24/05/13]
 27. Combating the Abuse of Alternative Remittance Systems (SR VI) Best Practice alternative remittance. <<http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalbestpracticescombatingtheabuseofalternativeremittancesystemssrvi.html>> [Accessed 24/05/13]
 28. Best Practice, cash couriers, bearer negotiable instruments (SR IX) <<http://www.fatf-gafi.org/documents/guidance/internationalbestpracticesdetectingandpreventingtheillicitcross-bordertransportationofcashandbearernegotiableinstrumentsrxi.html>> [Accessed 24/05/13]
 29. International Best Practices : Combating the abuse of Non -Profit Organisations. <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/11%20FATF%20SRIX%20BPP%20SRVIII%20October%202003%20-%20COVER%202012.pdf>> [Accessed 24/05/13]
 30. Guidance for financial institutions in detecting terrorist financing. <<http://www.fatf-gafi.org/media/fatf/documents/Guidance%20for%20financial%20institutions%20in%20detecting%20terrorist%20financing.pdf>> [Accessed 24/05/13]
 31. FATF [online] <<http://www.fatf-gafi.org/media/fatf/documents/reports/2000%202001%20NCCT%20ENG.pdf>> [Accessed 8 September 2013]
 32. FATF [online] <http://www.fatf-gafi.org/media/fatf/documents/reports/Initial%20Report%20on%20NCCTs%202002_2000.pdf> [Accessed 8 September 2013]
 33. FATF <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201996.pdf>> [Accessed 8 September 2013]

<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf>> [Accessed 8 September 2013]
 34. FATF <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf>> [Accessed 8 September 2013]

Wolfsberg Group AML Standards and Work

1. List of Wolfsburg Banks <http://www.wolfsberg-principles.com/index.html> [Accessed 27/05/13].
2. According to rel-banks 2013 as at end-March 2013 [online] Available at: <<http://www.relbanks.com/>> and also www.gfmag.com/tools/best-banks/11986-worlds-50biggest-banks-2012.html9x2eDqnj9BO
3. According to rel-banks 2013 as at end-April 2013 [online] Available at: <<http://www.relbanks.com/>>
4. See Part 1, Section 2, Sub-section 3, Products and Services Risks
5. Wolfsburg Group <http://www.wolfsberg-principles.com> [Accessed 27/05/13]
6. The Anti-Money Laundering (AML) Principles 2000/Global AML Guidelines for Private Banking 2002 (first revision) <http://www.wolfsberg-principles.com/pdf/Wolfsberg-Private-Banking-Principles-May-2012.pdf> accessed 28/05/13.
7. Wolfsburg Statement on the suppression of the financing of terrorist. [http://www.wolfsberg-principles.com/pdf/Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_\(2002\).pdf](http://www.wolfsberg-principles.com/pdf/Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_(2002).pdf) accessed 24/05/13.
8. Wolfsberg statement on corresponding banking principles. [http://www.wolfsberg-principles.com/pdf/Wolfsberg_Correspondent_Banking_Guidelines_\(2002\).pdf](http://www.wolfsberg-principles.com/pdf/Wolfsberg_Correspondent_Banking_Guidelines_(2002).pdf) accessed 24/05/13.
9. Statement on Monitoring Screening and Searching 2003 <http://www.wolfsberg-principles.com/monitoring.html> accessed 24/05/13
10. Bankers Almanac Due Diligence Repository 2004 <http://www.bankersalmanac.com/addcon/home/Submit-Documents.aspx> accessed 28/05/13.
11. Correspondent Banking FAQ's 2006 [http://www.wolfsberg-principles.com/pdf/Wolfsberg_Correspondent_Banking_FAQs_\(2006\).pdf](http://www.wolfsberg-principles.com/pdf/Wolfsberg_Correspondent_Banking_FAQs_(2006).pdf) accessed 28/05/13.
12. Guidance for Mutual Funds and other Pooled Investment Vehicles 2006. <http://www.wolfsberg-principles.com/mutual-funds.html> accessed 28/05/13.
13. Investment and Commercial Banking FAQ'S 2006. http://www.wolfsberg-principles.com/pdf/ibcb_faqs.pdf accessed 28/05/13.
14. Guidance on a Risk Based approach 2006. <http://www.wolfsberg-principles.com/risk-based-approach.html> accessed 28/05/13.
15. Statement against Corruption Guidance 2007 http://www.wolfsberg-principles.com/statement_against_corruption.html accessed 28/05/13.
16. Transparency of International Wire Transfers 2007. http://www.wolfsberg-principles.com/pdf/Cover_Payments_Press_Release_April-19-2007.pdf accessed 28/05/13.
17. FAQ's on PEP's revised and reissued 2008. [http://www.wolfsberg-principles.com/pdf/Wolfsberg_PEP_FAQs_\(2008\).pdf](http://www.wolfsberg-principles.com/pdf/Wolfsberg_PEP_FAQs_(2008).pdf) accessed 28/05/13.
18. Statement on Monitoring , Screening &Searching revised and reissued 2009. http://www.wolfsberg-principles.com/pdf/Wolfsberg_Monitoring_Screening_Searching_Paper-Nov_9_2009.pdf accessed 28/05/13.
19. Guidance on Credit Card Issuing and Merchant Acquiring Activities 2009. <http://www.wolfsberg-principles.com/credit-merchant.html> accessed 28/05/13.
20. Wolfsberg Anti-Corruption Guidance 2011. [http://www.wolfsberg-principles.com/pdf/Wolfsberg%20Anti%20Corruption%20Guidance%20Paper%20August%2018-2011%20\(Published\).pdf](http://www.wolfsberg-principles.com/pdf/Wolfsberg%20Anti%20Corruption%20Guidance%20Paper%20August%2018-2011%20(Published).pdf) accessed 28/05/13.
21. Trade Finance Principles 2009 and 2011. [http://www.wolfsberg-principles.com/pdf/Wolfsberg_Trade_Principles_Paper_II_\(2011\).pdf](http://www.wolfsberg-principles.com/pdf/Wolfsberg_Trade_Principles_Paper_II_(2011).pdf) accessed 28/05/13.
22. Guidance on Prepaid and Stored Value Cards 2011. http://www.wolfsberg-principles.com/pdf/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf accessed 28/05/13.
23. Private Banking Principles 2012: FAQ's on Intermediaries 2012 AND FAQ's on Beneficial Ownership 2012. <http://www.wolfsberg-principles.com/pdf/Wolfsberg-FAQs-on-Intermediaries-May-2012.pdf> <http://www.wolfsberg-principles.com/pdf/Wolfsberg-FAQs-on-Beneficial-Ownership-May-2012.pdf> accessed 28/05/13.

Sanctions & Embargoes

Introduction - Terrorism; Drug Trafficking and WMD

1. US Department of Treasury, Sanctions Programmes and Information [online] [2013]. Available at: <http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx> [Accessed 10 May 13]
2. Hendin, R., DEA Digging Into Al-Qaeda Drug Links, CBS News [online][2010]. Available at: <http://www.cbsnews.com>

- cbsnews.com/2100-500690_162-4274339.html (Accessed 10-May-13)
3. Bove-LaMonica, D. Polcymic, Al-Qaeda and Drug Trafficking, a Dangerous Partnership, [online][2011], Available at: <http://www.polcymic.com/articles/504/al-qaeda-and-drug-trafficking-a-dangerous-partnership> [Accessed 10 May 13]
 4. US Dept of Treasury Press Center, [online][2011], Available at: <http://www.treasury.gov/press-center/press-releases/pages/tg1057.aspx> (treasury website) [Accessed 10 May 13]
 5. Wikipedia, Definitions of Terrorism, [online][2013], Available at: http://en.wikipedia.org/wiki/Definitions_of_terrorism [Accessed 14-May-13]
 6. US State Dept. Archives, Patterns of Global Terrorism 1998, [online][1999], Available at: <http://www.higgin-sctc.org/patternsofglobalterrorism/1998pogr.pdf> [Accessed 14-May-13]
 7. UN Security Counsel, Resolution 1267 [online] [1999], Available at: [http://www.undemocracy.com/S-RES-1267\(1999\).pdf](http://www.undemocracy.com/S-RES-1267(1999).pdf) [Accessed 10 May 13]
 8. Wikipedia, September 11 Attacks, [online][2013], Available at: http://en.wikipedia.org/wiki/September_11_attacks [Accessed 14-May-13]
 9. UN Security Counsel Press Release SC/7158 [online][2001], Available at:<http://www.un.org/News/Press/docs/2001/sc7158.doc.htm> UNSCR 1373 [Accessed 10 May 13]
 10. Charbonneau, L., The UN Security Council Splits UN Sanctions List, Reuters, [online][2011], Available at : <http://www.reuters.com/article/2011/06/17/us-afghanistan-un-idUSTRE75G62720110617> [Accessed 14-May-13]
 11. UN Security Council, Resolution 1730-Delisting, [online][2006], <http://www.un.org/sc/committees/dfp.shtml> [Accessed 14-May-13]
 12. Wikipedia, Yasin al-Qadi, [online][2013], Availbe at: http://en.wikipedia.org/wiki/Yasin_al-Qadi [Accessed 14-May-13]
 13. US Treasury Dept. Office of Foreign Assets Control, Executive Order “Terrorism”, [online] [2001], Available at: <http://www.treasury.gov/resource-center/sanctions/programs/documents/terror.pdf> (EO 13224) [Accessed 10 May 13]
 14. Wikipedia, Patriot Act [online][2013], Available at: http://en.wikipedia.org/wiki/Patriot_Act [Accessed 14-May-13]
 15. US Treasury Dept., Office of Foreign Assets Control Guidance, [online] http://www.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf [Accessed 14-May-13]
 16. US Treasury Dept, OFAC, 2010 Terrorists Assets Report, [online][2010], Available at: <http://www.treasury.gov/resource-center/sanctions/Documents/tar2010.pdf> [Accessed 14-May-13]
 17. FATF GAFI, Text of the Special Recommendation and Interpretative Note, [online], Available at: [\http://www.un.org/en/sc/ctc/docs/bestpractices/fatf/9specialrec/9special-rec3.pdf [Accessed 14-May-13]
 18. US Treasury Dept, Resource Center [online][2012], Available at: <http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20130206.aspx> [Accessed 14-May-13]
 19. Seward & Kissell LLP, Iran Threat Reduction Act-SEC Disclosure Requirements, [online][2012], Available at: <http://www.sewkiis.com/pubs/xprPubDetail.aspx?xprST=PubDetail&pub=482> [Accessed 14-May-13]
 - 911 Civil Litigation Cases
 20. Hellerstein, A., The Upcoming 9/11 Trial Isn't About Money But Elusive Justice, Huff Post [online][2011], Available at: <http://www.huffingtonpost.com/perry-binder/9-11-trial_b_923234.html> [Accessed 10-May-13]
 21. Hellerstein, A., Managerial Judging: The 9/11 Responders Tort Litigation [online][Vol. 98:127], Available at: <http://www.lawschool.cornell.edu/research/cornell-law-review/upload/Hellerstein-et-al-final.pdf> [Accessed 10-May-13]
 22. History Commons, Complete 9/11 Timeline, [online], Available at: [http://www.historycommons.org/time-line.jsp?the_post-9/11_world=complete_911_timeline_9_11_related_lawsuits&timeline=complete_911_timeline] [Accessed 16-May-13]
 23. Wikipedia [online][2013], Available at: http://en.wikipedia.org/wiki/Cantor_Fitzgerald [Accessed 16-May-13]
 24. September 11th Victim's Compensation Fund, [online], Available at: <http://www.vcf.gov/> [Accessed 16-May-13]
 25. Ashcroft v. Iqbal, 490 F.3d 143 (2009) , Cornell University Law School [online], Available at <http://www.law.cornell.edu/supct/html/07-1015.ZS.html> [Accessed 10-May-13]
 26. Federal Register Vol. 60, No. 205, Executive Order 12978, [online][1995], Available at: <http://www.treasury.gov/resource-center/sanctions/Documents/12978.pdf> [Accessed 10-May-13]
 27. US Dept of Treasury, Office of Foreign Assets Control, Foreign Narcotics Kingpin Designation Act [online] [1995], Available at:<http://www.treasury.gov/resource-center/sanctions/Programs/Documents/drugs.pdf> (Accessed 10-May-13)

- 10-May-13)
28. Federal Register Vol. 60, No. 16, Executive Order 12947, [online][1995], Available at <http://www.treasury.gov/resource-center/sanctions/Documents/12947.pdf> [Accessed 10-May-13]
 29. US Treasury Dept., Office of Foreign Assets Control [online][1995], Available at: <http://www.treasury.gov/resource-center/sanctions/Documents/12978.pdf> [Accessed 10-May-13]
 30. White House Press Secretary Office, [online] [1999], Available at : http://www.whitehouse.gov/the_press_office/Fact-Sheet-Overview-of-the-Foreign-Narcotics-Kingpin-Designation-Act [Accessed 10-May-13]
 31. Spencer, B., Drug Certification, Foreign Policy on Focus, [online][1998] Available at: http://www.fpi.org/reports/drug_certification [Accessed 16-May-13]
 32. Wikipedia, Miguel Rodriguez Orejuela [online][2013] Available at: http://en.wikipedia.org/wiki/Miguel_Rodr%C3%ADguez_Orejuela [Accessed 16-May-13]
 33. OFAC Testimony Before the Oversight and Government Reform Subcommittee, June 24, 2011 [online][2011], Available at: http://oversight.house.gov/wp-content/uploads/2012/01/6-24-11_Szubin_Venezuela_Testimony.pdf [Accessed 16-May-13]
 34. US Dept of State, UN Security Council Resolution 1540 [online], Available at: <http://www.state.gov/t/isn/c18943.htm> [Accessed 10-May-13]
 35. US Treasury Dept, UN Security Council Resolution 1540 [online][2004], Available at:<http://www.treasury.gov/resource-center/sanctions/Documents/1540.pdf> [Accessed 10-may-13]
 36. Kraig, M. UN Seucity Council Resolution 1540 at the Crossroads: The Challenges of Implementation, the Standley Foundation, [online][2009], Available at: http://www.stimson.org/images/uploads/research-pdfs/The_Stanley_Foundation_Report_-_The_Challenges_of_Implementation.pdf [accessed 16-may-13]
 37. US Dept of Treasury, Office of Foreign Assets Control, 31 CFR 539 [online][1999], Available at: <http://www.gpo.gov/fdsys/pkg/FR-1999-02-23/pdf/99-4328.pdf> [Accessed 16-May-13]
 38. US Treasury Dept, Office of Foreign Assets Control, Executive Order 13382 [online][2005], Available at: <http://www.treasury.gov/resource-center/sanctions/Programs/Documents/wmd.pdf> [Accessed 10-May-13]
 39. Wikipedia, Megatons to Megawatts Programme [online][2008], Available at:http://en.wikipedia.org/wiki/Megatons_to_Megawatts_Program [Accessed 10-May-13]
 40. Federal Register, Vol. 65, No. 123, June 26, 2000, Executive Order 13159 [online][2000], Available at: <http://www.gpo.gov/fdsys/pkg/FR-2000-06-26/pdf/00-16252.pdf> [Accessed 16-May-13]

Country Programmes - Belarus; DRC; Iran and Myanmar

1. Stern, D., West wrings hands over Belarus, GlobalPost [online][2011], Available at <http://www.globalpost.com/dispatch/belarus/110101/2010-presidential-election-crackdown> [Accessed 10-May-13]
2. Wikipedia, Belarusian presidential election, 2010 [online][2013], Available at:http://en.wikipedia.org/wiki/Belarusian_presidential_election,_2010 [Accessed 10-May-13]
3. Kramer, D. Europe's last dictator, The Washington Post [online][2011], Available at:http://articles.washingtonpost.com/2011-07-08/opinions/35267018_1_alexander-lukashenko-street-protests-human-rights-abuses [Accessed 10-May-13]
4. Gov.UK, Embargoes and sanctions on Belarus [online][2012], Available at:<https://www.gov.uk/arms-embargo-on-belarus> [Accessed 10-May-13]
5. Castle, St. EU Temporarily Suspends Travel Ban for Belarussian Leader, The New York Time [online][2008], Available at: <http://www.nytimes.com/2008/10/14/world/europe/14belarus.html> [Accessed 10-May-13]
6. State Secretariat For Economic Affairs, Sanctions measures against Belarus [online][2006], Available at:<http://www.seco.admin.ch/aktuell/00277/01164/01980/index.html?lang=en&msg-id=5885> [Accessed 10-May-13]
7. Belarus News and Analysis, US Extends Travel Ban to More Belarussian Officials As Minsk Threatens to Retaliate [online][2007], Available at: <http://www.data.minsk.by/belarusnews/082007/201.html> [Accessed 10-May-13]
8. State Secretariot for Economic Affairs, Sanctions Measures Against Belarus,] [online][2006], Available at: <http://www.seco.admin.ch/aktuell/00277/01164/01980/index.html?lang=en&msg-id=5885> [Accessed 16-May-13]
9. BBC News, Russian warns of Belarus missiles [online][2007], Available at:<http://news.bbc.co.uk/2/hi/europe/7094347.stm> [Accessed 10-May-13]
10. US Treasury Dept, Treasury Sanctions Four Entities of Major State-Owned Belarusian Petrochemicals Conglomerate [online][2011], Available at: http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/belarus_notice_08112011.pdf [Accessed 10-May-13]
11. UN News Centre, Security Council renews arms embargo and sanctions in DR Congo, [online][2011], Available at: <http://www.un.org/apps/news/story.asp?NewsID=40563> [Accessed 10-May-13]

12. Global Policy Forum, Democratic Republic of Congo [online][2013], Available at:<http://www.globalpolicy.org/security-council/index-of-countries-on-the-security-council-agenda/democratic-republic-of-congo.html> [Access 10-May-13]
13. Wikipedia, Democratic Republic of Congo [online][2013], Available at:http://en.wikipedia.org/wiki/Democratic_Republic_of_the_Congo [Accessed 10-May-13]
14. UN Security Council, Resolution 1493 [online][2003], Available at:<http://watchlist.org/wordpress/wp-content/uploads/SCR-1493-DRC-sanctions-committee.pdf> [Accessed 10-May-13]
15. Wikisource, UN Security Council Resolution 1533 [online][2004], Available at: http://en.wikisource.org/wiki/United_Nations_Security_Council_Resolution_1533 [Accessed 10-May-13]
16. UN, Resolution 1533 [online][2013], Available at: <http://www.un.org/sc/committees/1533/> [Accessed 10-May-13]
17. Wikipedia, UNSCR 1952, [online][2013], Available at: http://en.wikipedia.org/wiki/United_Nations_Security_Council_Resolution_1952 [Accessed 10-May-13]
18. Sanctions Wiki, Democratic Republic Congo [online][2013], Available at: http://www.sanctionswiki.org/Democratic_Republic_of_the_Congo [Accessed 10-May-13]
19. US Securities and Exchange Commission, SEC Adopts Rule for Disclosing Use of Conflict Minerals [online] [2012], Available at: <http://www.sec.gov/news/press/2012/2012-163.htm> [Accessed 10-May-13]
- CUBA
20. Wikipedia, US embargo against Cuba [online][2013], Available at: http://en.wikipedia.org/wiki/United_States_embargo_against_Cuba [Accessed 10-May-13]
21. Wikipedia, Helms-Burton Act [online][2013], Available at: http://en.wikipedia.org/wiki/Helms%20Burton_Act [Accessed 10-May-13]
22. Wikipedia, National Liberation Army (Colombia) [online][2013], Available at:[http://en.wikipedia.org/wiki/National_Liberation_Army_\(Colombia\)](http://en.wikipedia.org/wiki/National_Liberation_Army_(Colombia)) [Accessed 10-May-13]
23. Torregrosa, L., Obama Lifts Some Cuba Travel Restrictions, Huffpost Politics-Politics Daily [online][2012], Available at: <http://www.politicstoday.com/2011/01/15/some-cuba-travel-restrictions-are-lifted/> [Accessed 10-May-13]
24. Wikipedia, 2006-07 Economic Sanctions Against Palestinian National Authority [online][2013], Available at: http://en.wikipedia.org/wiki/2006%E2%80%9307_economic_sanctions_against_the_Palestinian_National_Authority [Accessed 10-May-13]
25. Wikipedia, Hamas [online][2012], Available at: <http://en.wikipedia.org/wiki/Hamas> [Accessed 10-May-13]
26. Wikipedia, Salam Fayyad [online][2013], Available at: https://en.wikipedia.org/wiki/Salam_Fayyad [Accessed 10-May-13]
27. Hamas: Baclgrpmid & Issues for Congress, Congressor, Research Office [online] [2010], Available at: <<http://www.fas.org/sgp/crs/mideast/R41514.pdf>> [Accessed 29 August 13]
28. Linde v. Arab Bank, PLC, 269 F.R.D. 186 (2010), Thomson Reuters [online][2013], Available at: http://newsandinsight.thomsonreuters.com/uploadedFiles/Reuters_Content/2013/01_-_January/Linde%20v%20Arab%20Bank%20PLC.pdf [Accessed 10-May-13]
29. Linde v. Arab Bank, 10-cv-4519 (2013), FindLaw, [online][2013], Available at: Linde v. Arab Bank, 10-cv-4519, [Accessed 17-May-13]
30. Applied Discovery Online Law Library, Weiss v. National Westminster Bank, PLC, 2007 US Dist. Lexis 35103 (E.D.N.Y. May 14, 2007), [online][2013], Available at: http://www.applieddiscovery.com/ws_display.asp?filter=Case%20Summaries%20Detail&item_id=%7B897E6319-B26A-4DE4-A885-65F48041C1AF%7D [Accessed 10-May-13]
31. Smythe, C., Credit Lyonnais Suit Over Middle East Attacks Nears Trial, Bloomberg [online][2013], Available at: <http://www.bloomberg.com/news/2013-03-01/credit-lyonnais-suit-over-middle-east-attacks-nears-trial.html> [Accessed 10-May-13]
32. Swinger, R., Bank Potentially Liable or Terrorist Attacks, Financial Services Litigation Newswire [online] [2011], Available at: http://www.chadbourne.com/files/publication/9711e556-66c4-492a-a138-b08202caed2/presentation/publicationattachment/b4bf6e1a-2d51-4930-b82c-b131370c5ad4/FSL_Newswire_Sept2011.pdf [Accessed 10-May-13]
33. Pierson, B., Suit Accusing Arab Bank of Supporting Terrorism Is Dismissed, Law.Com [online] [2012], Available at: http://www.law.com/jsp/article.jsp?id=1202577634480&Suit_Accusing_Arab_Bank_of_Supporting_Terrorism_Is_Dismissed&slsreturn=20130417111402 [Accessed 17-May-13]
34. Wikipedia, Sanctions Against Iran [online][2013], Available at: http://en.wikipedia.org/wiki/Sanctions_against_Iran [Accessed 13-May-13]
35. Smith Anderson, New Reporting Requirements Under the Iran Threat Reduction and Syria Human Rights Act of 2012, [online][2013], Available at: <http://www.smithlaw.com/updates-alerts-199.html> [Accessed 13-May-13]
36. Wikipedia, State Sponsors of Terrorism, [online][2013], Available at: http://en.wikipedia.org/wiki/State_Sponsors_of_Terrorism [Accessed 17-May-13]
37. Murphy, B., Iran and Al-Qaeda Connected? The History Behind A Complex Relationship, Huff Post World [online][2013], Available at: http://www.huffingtonpost.com/2013/04/23/iran-al-qaeda_n_3139749.html [Accessed 13-May-13]
38. The Soufan Group, TSG IntelBrief: The Qods Force: Spearheading Iran's Foreign Policy, [online][2013], Available at: http://soufangroup.com/briefs/details/?Article_Id=513 [Accessed 13-May-13]
39. Wikipedia, Hezbollah Foreign Relations, [online][2013], Available at:http://en.wikipedia.org/wiki/Hezbollah_foreign_relations [Accessed 13-May-13]
40. Wikipedia, Iran-US Relations, [online][2013], Available at : http://en.wikipedia.org/wiki/Iran%E2%80%93United_States_relations [Accessed 13-May-13]
41. Wikipedia, US Sanctions Against Iran, [online][2013], Available at: http://en.wikipedia.org/wiki/US_sanctions_against_Iran [Accessed 13-May-13] http://en.wikipedia.org/wiki/Iran%E2%80%93United_States_relations
42. Wikipedia, Iran-US Relations, [online][2013], Available at: http://en.wikipedia.org/wiki/Iran%E2%80%93United_States_relations [Accessed 13-May-13]
43. Katzman, K., The Iran-Libya Sanctions Act (ILSA), CRS Report for Congress [online][2003], Available at:http://www.parstimes.com/law/ilsa_extension2003.pdf [Accessed 14-May-13]
44. Davidson, N., US Secondary Sanctions: The UK and EU Response, [online], Available at: <http://www.law.stetson.edu/lawreview/media/u-s-secondary-sanctions-the-u-k-and-e-u-response.pdf> [Accessed 13-May-13]
45. Croft, A., EU Warns of WTO Move if US Imposes Sanctions, [online][1998], Available at: <http://www.cubanet.org/CNews/y98/may98/27e3.htm> [Accessed 13-May-13]
46. Hearing before the Subcommitee on the Middle East and Central Asia, Enforcmenet of the Iran Lybia Sanctions Act, [online][2003], Avilable at: http://commdocs.house.gov/committees/intrel/hfa87998.000/hfa87998_0.htm [Accessed 17-May-13]
47. Katzman, K., Iran Libay Sanctions Act, CRS Report for Congress, [online][2005], Available at: <http://fpc.state.gov/documents/organization/64937.pdf> [Accessed 13-May-13]
48. Public Intelligence, Iran Nuclear Site: Natanz Uranium Enrichment Site [online][2010], Available at: <http://publicintelligence.net/iran-nuclear-site-natanz-uranium-enrichment-site/> [Accessed 13-May-13]
49. Wikipedia, Timeline of the Nuclear Programme in Iran, [online][2013], Available at: http://en.wikipedia.org/wiki/Timeline_of_the_nuclear_programme_of_Iran [Accessed 13-May-13]
50. UN, Security Counsel SC/9948 [online][2010], Available at:<http://www.un.org/News/Press/docs/2010/sc9948.doc.htm> [Accessed 13-May-13]
51. US Institute of Peace, New US Sanctions on Iran Air and Others, [online][2011], Available at: <http://iranprimer.usip.org/blog/2011/jun/23/new-us-sanctions-iran-air-and-others> [Accessed 14-May-13]
52. Winston & Strawn LLP, Treasury Denies Three Iranian Banks Access to the US Financial System, [online] [2007], Available at: http://winston.com/siteFiles/publications/Iranian_Banks_Denied_Access.pdf [Accessed 13-May-13]
53. Levitt, M., Disrupting Tehran's Export of Technology and Weapons, The Washington Institute [online][2009], Available at: <http://www.washingtoninstitute.org/policy-analysis/view/disrupting-tehrans-export-of-technology-and-weapons> [Accessed 17-May-13]
54. US Treasury Dept., Designation of Six IRISL Fronts [online][2011], Available at: http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/irisl_panama_notice_10272011.pdf [Accessed 13-May-13]
55. McCain, N., 16 Charged with Iran Trade Embargo Crimes, Courthouse News Service [online][2011], Available at: <http://www.courthousenews.com/2011/06/20/37529.htm> [Accessed 13-May-13]
56. DeYoung, K., US, Allies Say Iran Has Secret Nuclear Facility, The Washington Post [online][2009], Available at: http://articles.washingtonpost.com/2009-09-26/world/36784470_1_secret-nuclear-facility-qom-facility-enrichment [Accessed 13-May-13]
57. http://en.wikipedia.org/wiki/United_Nations_Security_Council_Resolution_1929 Official Journal of the European Union, Council Regulation (EU) No 961/2010, [online][2010], Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:281:0001:0077:EN:PDF> [Accessed 13-May-13]
58. Official Journal of the European Union, Counceil Regulation (EU) No 961/2010, [online][2010], Available at:

[\[Accessed 13-May-13\]](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:281:0001:0077:EN:PDF)

59. Slater, J., Swiss-Iranian relations take a new track, Swiss Broadcasting Corp, [online][2011], Available at: http://www.swissinfo.ch/eng/politics/Swiss-Iranian_relations_take_a_new_track.html?cid=29306360 [Accessed 13-May-13]

60. State Secretariat for Economic Affairs, Iran: Federal Council takes steps to improve legal certainty and prevent possible evasion, [online][2011], Available at: http://www.seco.admin.ch/aktuell/00277/01164/01980/?lang=en&cm_sg-id=37283 [Accessed 13-May-13]

61. Wikipedia, Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010, [online][2013], Available at: http://en.wikipedia.org/wiki/Comprehensive_Iran_Sanctions,_Accountability,_and_Divestment_Act_of_2010 [Accessed 13-May-13]

62. Govtrack, HR 1905 (112th): Iran Threat Reduction and Syria Human Rights Act of 2012, [online][2012], Available at: <http://www.govtrack.us/congress/bills/112/hr1905/text> [Accessed 13-May-13]

63. Smith Anderson, New Reporting Requirements Under the Iran Threat Reduction and Syria Human Rights Act of 2012, [online][2013], Available at: <http://www.smithlaw.com/updates-alerts-199.html> [Accessed 13-May-13]

64. Eur Lex, European Union on Burma/Myanmar, [online][1996], Available at: <http://www.google.com/hostednews/afp/article/ALeqM5gLXdk1i3Gfy5eZ8RPB8F8agCpPjg?docId=CNG.a86eb6b2701ce148592ac01588b-748be.781> [Accessed 14-May-13]

65. Economic Sanctions Against Burma: Human Right Issue and Congressional Initiative, [online][1997], Available at: http://www.yemyint88.net/Eco_Sanctions_SLORC.pdf [Accessed 14-May-13]

66. Burmese Freedom and Democracy Act of 2003, Public Law 108-61 July 28, 2003, [online][2003], Available at: http://www.treasury.gov/resource-center/sanctions/Documents/bfda_2003.pdf [Accessed 14-May-13]

67. US Dept. of State Archive, Burmese Freedom and Democracy Act of 2003 and Executive Order, [online][2003], Available at: <http://2001-2009.state.gov/p/eap/rls/rm/2003/22851.htm> [Accessed 14-May-13]

68. Wikipedia, 2007 Burmese anti-government protests, [online][2013], Available at: http://en.wikipedia.org/wiki/2007_Burmese_anti-government_protests [Accessed 14-May-13]

69. US Treasury Dept., Office of Foreign Assets Control-Burma [online][2008], Available at: <http://www.treasury.gov/resource-center/sanctions/Documents/burma.pdf> [Accessed 14-May-13]

70. Sanctions Wiki, Myanmar [online][2013], Available at: <http://www.sanctionswiki.org/Myanmar> [Accessed 14-May-13]

71. BBC News, Overview of Burma Sanctions, [online][2009], Available at: <http://news.bbc.co.uk/2/hi/asia-pacific/8195956.stm> [Accessed 14-May-13]

72. BBC News, Who Maintains Sanctions on Burma? [online][2010], Available at: <http://www.bbc.co.uk/news/world-asia-pacific-11551130> [Accessed 14-May-13]

73. Wikipedia, Golden Triangle (Southeast Asia), [online][2013], Available at: [http://en.wikipedia.org/wiki/Golden_Triangle_\(Southeast_Asia\)](http://en.wikipedia.org/wiki/Golden_Triangle_(Southeast_Asia)) [Accessed 14-May-13]

74. Energy Giants 'fund Burmas nuclear drive', BurmaPartnership, [online][2010] <http://www.burmapartnership.org/2010/07/energy-giants-fund-burmas-nuclear-drive/> [Accessed 17-May-13]

75. Corridor of Power: China's Trans-Burma Oil and Gas Pipelines, Shwe Gas Movement, [online][2009], Available at: <http://www.shwe.org/wp-content/uploads/2011/03/CorridorofPower.pdf> [Accessed 17-May-13]

76. US Government Keeps Watch over Burma's Nuclear Programme, Institute for Science and International Security (ISIS), [online][2010], Available at: <http://isis-online.org/isis-reports/detail/u.s.-government-keeps-watch-over-burmas-nuclear-program/> [Accessed 17-May-13]

77. Hughes, D., Obama Administration Declares Myanmar Open For Business, ABC News, [online][2012], Available at: <http://abcnews.go.com/blogs/politics/2012/05/obama-administration-declares-myanmar-open-for-business/> [Accessed 17-May-13]

78. Squire Sanders, US Eases Finance Services and Investment Sanctions Against Myanmar-With Conditions, [online][2012], Available at: <http://www.squiresanders.com/files/Publication/96d3be8a-a9cc-4be9-82d7-b75e76024aae/Presentation/PublicationAttachment/62fc467b-d8db-4e7c-b3b1-b7be8181c48a/US-Eases-Financial-Services-and-Investment-Sanctions-Against-Myanmar-with-conditions.pdf> [Accessed 17-May-13]

79. Wikipedia, Economy of Burma, [online][2013], Available at: http://en.wikipedia.org/wiki/Economy_of_Burma [Accessed 17-May-13]

80. Rosenberg, C., EU Suspends Most Sanctions Against Myanmar, AFP, [online][2012], Available at: <http://www.google.com/hostednews/afp/article/ALeqM5gLXdk1i3Gfy5eZ8RPB8F8agCpPjg?docId=CNG.a86eb6b2701ce148592ac01588b-748be.781> [Accessed 14-May-13]

81. Burma Partnership <http://www.burmapartnership.org/tag/us-campaign-for-burma/>

Country Programmes - North Korea; Sudan; Syria; Venezuela and Zimbabwe

1. CNN World, UN slaps trade, travel sanctions on North Korea, [online][2006], Available at: <http://www.cnn.com/2006/WORLD/asiapcf/10/14/nkorea.sanctions/> [Accessed 20-May-13]
2. CRS Report for Congress, North Korea: Economic Sanctions, [online][2006], Available at: <http://www.fas.org/sgp/crs/row/RL31696.pdf> [Accessed 20-May-13]
3. US Dept of Treasury, Office of Foreign Assets Control, North Korea: An Overview of Sanctions With Respect to North Korea, [online][2011], Available at: <http://www.treasury.gov/resource-center/sanctions/Programs/Documents/nkorea.pdf> [Accessed 20-May-13]
4. Paddock, R., N. Koea's Growing Drug Trade Seen in Botched Heroin Delivery, The Los Angeles Times, [online][2003], Available at: <http://articles.latimes.com/2003/may/21/world/fg-heroin21> [Accessed 20-May-13]
5. Arms Control Association, The Six-Party Talks at a Glance, [online][2012], Available at: <http://www.armscontrol.org/factsheets/6partytalks> [Accessed 20-May-13]
6. Bajoria, J., The Six-Party Talks on North Korea's Nuclear Programme, Council on Foreign Relations, [online][2013], Available at: <http://www.cfr.org/proliferation/six-party-talks-north-koreas-nuclear-program/p13593> [Accessed 20-May-13]
7. UN Security Council SC/8853, Security Council Condemns Nuclear Test by Democratic People's Republic of Korea, Unanimously Adopting Resolution 1718 (2006, [online][2006], Available at: <http://www.un.org/News/Press/docs/2006/sc8853.doc.htm> [Accessed 20-May-13]
8. Sanctions Wiki, North Korea, [online][2013], Available at: http://www.sanctionswiki.org/North_Korea [Accessed 20-May-13]
9. Associated Press, North Korea agrees to nuclear disarmament, NBC News [online][2007], Available at: http://www.nbcnews.com/id/17117242/ns/world_news-asia_pacific/t/north-korea-agrees-nuclear-disarmament/ [Accessed 20-May-13]
10. Gard, R., Lt. General, Negotiating with North Korea on its Nuclear Programme, The Center for Arms Control and Non-Proliferation, [online][2011], Available at: http://armscontrolcenter.org/issues/northkorea/articles/negotiating_with_north_korea_on_its_nuclear_program/ [Accessed 20May-13]
11. Wikipedia, 2009 North Korean missile test, [online][2013], Available at: http://en.wikipedia.org/wiki/2009_North_Korean_missile_test [Accessed 20-May-13]
12. Nikitin, M., North Korea's Second Nuclear Test: Implications of UN Security Council Resolution 1874, Congressional Research Service, [online][2010], Available at: <http://www.fas.org/sgp/crs/nuke/R40684.pdf> [Accessed 20-May-13]
13. Wikipedia, UN Security Council Resolution 1874, [online][2013], Available at: http://en.wikipedia.org/wiki/United_Nations_Security_Council_Resolution_1874 [Accessed 20-may-13]
14. Rogin, J., Obama goes after Kim Jong Il's creature comforts, Foreign Policy, [online][2010], Available at: http://thecable.foreignpolicy.com/posts/2010/08/30/obama_goes_after_kim_jong_il_s_creature_comforts
15. Cho, J., 'Obvious' North Korea Sank South Korean Ship, ABC News, [online][2010], Available at: <http://abcnews.go.com/International/obvious-north-korea-sank-south-korean-ship/story?id=10685652> [Accessed 20-May-13]
16. Lynch, C., Security Council to release long-delayed North Korea nuclear report, Washington Post, [online][2010], Available at: <http://www.washingtonpost.com/wp-dyn/content/article/2010/11/09/AR2010110907180.html> [Accessed 20-May-13]
17. US Treasury Dept., Office of Foreign Assets Control, Sudan Sanctions [online][2008], Available at: <http://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf> [Accessed 20-May-13]
18. Schanzer, J., Pariah State: Examining Sudan's Support for Terrorism, Foundation for Defense of Democracies, [online][2012], Available at: <http://www.defenddemocracy.org/media-hit/pariah-state-examining-sudans-support-for-terrorism/> [Accessed 20-May-13]
19. Wikipedia, War in Darfur, [online][2013], Available at: http://en.wikipedia.org/wiki/War_in_Darfur [Accessed 20-May-13]
20. UN Security Council Press Release, Security Council Imposes Travel Ban, Assets Freeze, [online][2005], Available at: <http://www.un.org/News/Press/docs/2005/sc8346.doc.htm> [Accessed 20-May-13]
21. Sanctions Wiki, Sudan, [online][2013], Available at: <http://www.sanctionswiki.org/Sudan> [Accessed 20-May-13]
22. Wikipedia, Second Sudanese Civil War, [online][2013], Available at: http://en.wikipedia.org/wiki/Second_Sudanese_Civil_War [Accessed 20-May-13]

23. Wikipedia, South Sudan, [online][2013], Available at: http://en.wikipedia.org/wiki/South_Sudan [Accessed 20-May-13]
24. US Treasury Dept, Embassy of the US, Doing Business with South Sudan, [online][2011], Available at: <http://southsudan.usembassy.gov/business/doing-business-in-south-sudan.html> [Accessed 20-May-13]
25. Holland, H., Aerial bombardment and ground attacks by government forces in Sudan. . .amount to war crimes, Reuters, [online][2013], Available at: <http://www.reuters.com/article/2013/01/21/us-sudan-border-idUSBRE90K-0KL20130121> [Accessed 20-May-13]
26. Wikipedia, Timeline of the Syrian Civil War, [online][2013], Available at: [http://en.wikipedia.org/wiki/Timeline_of_the_Syrian_civil_war_\(January%20to%20April_2011\)](http://en.wikipedia.org/wiki/Timeline_of_the_Syrian_civil_war_(January%20to%20April_2011)) [Accessed 20-May-13]
27. International Sanctions on Syria, EUBusiness, [online][2012], Available at: <http://www.eubusiness.com/news-eu/syria-politics.htm> [Accessed 20-May-13]
28. CBC News World, EU bans oil imports from Syria, [online][2011], Available at: <http://www.cbc.ca/news/world/story/2011/09/02/syria-sanctions.html> [Accessed 21-May-13]
29. Covington & Burling LLP E-Alert, EU Widens the Scope fo Sanctions Against Syria and Iran, [online] [2011], <http://www.cov.com/files/Publication/202446fd-6d92-4531-8347-c57c4f3f48f7/Presentation/PublicationAttachment/68c432c5-c060-45b3-bca2-d3373ba66e77/EU%20Widens%20the%20Scope%20of%20Sanctions%20Against%20Syria%20and%20Iran.pdf> [Accessed 21-May-13]
30. US Treasury Dept, Executive Order 13582 of August 17, 2011, [online][2011], Available at: http://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_eo_08182011.pdf [Accessed 21-May-13]
31. US State Dept, Country Reports on Terrorism 2010, [online][2011], Available at: <http://www.state.gov/j/ct/rls/crt/2010/170260.htm> [Accessed 21-May-13]
32. CNN International, US hits Syria with sanctions, [online][2004], Available at: <http://edition.cnn.com/2004/WORLD/meast/05/11/us.syria/> [Accessed 21-May-13]
33. Wikipedia, UN Security Council Resolution 1636, [online][2012], Available at: http://en.wikipedia.org/wiki/United_Nations_Security_Council_Resolution_1636 [Accessed 21-May-13]
34. Associated Press, US imposes sanctions on Syrian businessman, NBC News [online][2008], Available at: http://www.nbcnews.com/id/23277636/ns/world_news-mideast_n_africa/t/us-imposes-sanctions-syrian-businessman/ [Accessed 21-May-13]
35. The Guardian, Syrian nuclear weapons site revealed by UN investigators, [online][2011], Available at: <http://www.guardian.co.uk/world/2011/nov/01/syria-nuclear-weapons-site-revealed> [Accessed 21-May-13]
36. US State Dept., Country Reports on Terrorism 2009, [online][2010], Available at: <http://www.state.gov/j/ct/rls/crt/2009/140889.htm> [Accessed 21-May-13]
37. US State Dept., Iran Sanctions Contained in the Iran Threat Reduction and Syria Human Rights Act, [online][2010], Available at: <http://www.state.gov/e/eb/rls/fs/2012/198393.htm> [Accessed 21-May-13]
38. Oversight and Government Reform Subcommittee, Written Testimony by US Treasury Dept. OFAC Director, Venezuela's Sanctionable Activity, [online][2011], Available at: [onlihttp://archives.republicans.foreignaffairs.house.gov/112/szu062411.pdf](http://archives.republicans.foreignaffairs.house.gov/112/szu062411.pdf) [Accessed 21-May-13]
39. US Government Accounting Office, Drug Control, US Counternarcotics Cooperation with Venezuela Has Declined, [online][2009], Available at: <http://www.gao.gov/new.items/d09806.pdf> [Accessed 21-May-13]
40. CNN International, US sanctions Venezuelan officials for allegedly helping FARC rebels, [online][2011], Available at: <http://edition.cnn.com/2011/WORLD/americas/09/08/venezuela.ofac.list/index.html> [Accessed 22-May-13]
41. Wikipedia, Revolutionary Armed Forces of Colombia, [online][2013], Available at: http://en.wikipedia.org/wiki/Revolutionary_Armed_Fores_of_Colombia [Accessed 22-May-13]
42. Phillips, J., US Treasury Sanctions Four High-Level Venezuelan Officials, The Epoch Times, [online][2011], Available at: <http://www.theepochtimes.com/n2/world/us-treasury-sanctions-four-high-level-venezuelan-officials-61383.html> [Accessed 22-May-13]
43. US Treasury Dept., Press Center, Treasury Targets Venezuelan Government Officials Supporting the FARC, [online][2008], Available at: <http://www.treasury.gov/press-center/press-releases/Pages/hp1132.aspx> [Accessed 22-May-13]
44. Frieden, T., US: Two Venezuelans are supporting terrorism, CNN World, [online] [2008], Available at: <http://edition.cnn.com/2008/WORLD/meast/06/18/venezuela.hezbollah/> [Accessed 22-May-13]
45. Reuters, Colombia Ties Drug Ring to Hezbollah, The New York Times, [online][2008], Available at: http://www.nytimes.com/2008/10/22/world/americas/22colombia.html?_r=0 [Accessed 22-May-13]
46. Morgenthau, R., The Link Between Iran and Venezuela—A Crisis int eh Making?, The Herald Tribune, [online]
- [20009], Available at: <http://laht.com/article.asp?ArticleId=343289&CategoryId=10718> [Accessed 22-May-13]
47. Wikipedia, Iran—Venezuela relations, [online][2013], Available at: http://en.wikipedia.org/wiki/Iran%E2%80%93Venezuela_relations [Accessed 22-May-13]
48. Mahjar-Barducci, A., Iran Placing Medium-Range Missiles in Venezuela; Can Reach the US, Gatestone Institute, [online][2010], Availalbe at: <http://www.gatestoneinstitute.org/1714/iran-missiles-in-venezuela> [Accessed 22-May-13]
49. The New York Times, Venezuela Affirms/Denies Iran is Helping it look for Uranium, The Obama Report, [online][2009], Available at: The New http://obamareport.blogspot.com/2009_09_01_archive.html [Accessed 22-May-13]
50. Wikipedia, Robert Mugabe, [online][2013], Available at: http://en.wikipedia.org/wiki/Robert_Mugabe [Accessed 22-May-13]
51. Zimbabwe Democracy and Economic Recovery Act of 2001, Public Law 107-99, Dec. 21, 2001 [online] [2001], Available at: <https://bulk.resource.org/gpo.gov/laws/107/publ099.107.pdf> [Accessed 22-May-13]
52. Sanctions Wiki, Zimbabwe, [online][2013], Available at: <http://www.sanctionswiki.org/Zimbabwe> [Accessed 22-May-13]
53. Jeuck, L., Arms Transfers to Zimbabwe: Implications for an Arms Trade Treaty, Sipri [online][2011], Available at: <http://books.sipri.org/files/misc/SIPRIBP1103.pdf> [Accessed 22-May-13]
54. Ploch, L., Zimbabwe: The Power Sharing Agreement and Implications for US Policy, Congressional Research Service, [online][2009], Available at: <http://fpc.state.gov/documents/organization/125502.pdf> [Accessed 22-May-13]

Part 1, Section 4 - Money Laundering Prevention Programmes

1. FATF: Available at: <<http://www.fatf.com>> [Accessed 14 July 2013]. See also Part 1, Section 3, Money Laundering Laws and Regulations; Financial Action Task Force.

Risk Assessment

1. Bank for International Settlements. 2013. 'Sound management of risks related to money laundering and financing of terrorism - consultative document' June 2013 [online] Available at: <<http://www.bis.org/publ/bcbs252.htm>> [Accessed 14 July 2013]

2. FFEIC Manual - [online] Available at: <http://www.ffeic.gov/bsa_aml_infobase/pages_manual/OLM_005.htm> [Accessed 24 July 2013]. According to the FFEIC Manual, "a well-developed risk assessment will assist in identifying the bank's BSA/AML risk profile. Understanding the risk profile enables the bank to apply appropriate risk management processes to the BSA/AML compliance programme to mitigate risk. This risk assessment process enables management to better identify and mitigate gaps in the bank's controls. The risk assessment should provide a comprehensive analysis of the BSA/AML risks in a concise and organised presentation and should be shared and communicated with all business lines across the bank, board of directors, management, and appropriate staff; as such, it is a sound practice that the risk assessment be reduced to writing. There are many effective methods and formats used in completing a BSA/AML risk assessment; therefore, examiners should not advocate a particular method or format. Bank management should decide the appropriate method or format, based on the bank's particular risk profile. Whatever format management chooses to use for its risk assessment, it should be easily understood by all appropriate parties. The development of the BSA/AML risk assessment generally involves two steps: first, identify the specific risk categories (i.e., products, services, customers, entities, transactions, and geographic locations) unique to the bank; and second, conduct a more detailed analysis of the data identified to better assess the risk within these categories." The FFEIC Manual also states that...." in reviewing the risk assessment during the scoping and planning process, the examiner should determine whether management has considered all products, services, customers, entities, transactions, and geographic locations, and whether management's detailed analysis within these specific risk categories was adequate. If the bank has not developed a risk assessment, this fact should be discussed with management. For the purposes of the examination, whenever the bank has not completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment based on available information." The FFEIC manual then goes on to say that..."An examiner must review the bank's BSA/AML compliance programme with sufficient knowledge of the bank's BSA/AML risks in order to determine whether the BSA/AML compliance programme is adequate and provides the controls necessary to mitigate risks. For example, during the examination scoping and planning process, the examiner may initially determine that the bank has a high-risk profile, but during the examination, the examiner may determine that the bank's BSA/AML compliance programme adequately mitigates these risks. Alternatively, the examiner may initially determine that

the bank has a low- or moderate- risk profile; however, during the examination, the examiner may determine that the bank's BSA/AML compliance programme does not adequately mitigate these risks."....and, "In evaluating the risk assessment, an examiner should not necessarily take any single indicator as determinative of the existence of a lower or higher BSA/AML risk. The assessment of risk factors is bank-specific, and a conclusion regarding the risk profile should be based on a consideration of all pertinent information. Banks may determine that some factors should be weighed more heavily than others. For example, the number of funds transfers is certainly one factor to be considered in assessing risk; however, in order to effectively identify and weigh the risks, the examiner should look at other factors associated with those funds transfers, such as whether they are international or domestic, the dollar amounts involved, and the nature of the customer relationships." The Manual then goes on to identify specific risk factors and states....."the first step of the risk assessment process is to identify the specific products, services, customers, entities, and geographic locations unique to the bank. Although attempts to launder money, finance terrorism, or conduct other illegal activities through a bank can emanate from many different sources, certain products, services, customers, entities, and geographic locations may be more vulnerable or have been historically abused by money launderers and criminals. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered...the differences in the way a bank interacts with the customer (face-to-face contact versus electronic banking) also should be considered." On products and services, the Manual states that..."Certain products and services offered by banks may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services are listed below, but the list is not all inclusive: Electronic funds payment services — electronic cash (e.g., prepaid and payroll cards), funds transfers (domestic and international), payable upon proper identification (PUPID) transactions, third-party payment processors, remittance activity, automated clearing house (ACH) transactions, and automated teller machines (ATM). Electronic banking; Private banking (domestic and international); Trust and asset management services; Monetary instruments; Foreign correspondent accounts (e.g., bulk shipments of currency, pouch activity, payable through accounts (PTA), and U.S. dollar drafts); Trade finance; Services provided to third party payment processors or senders; Foreign exchange; Special use or concentration accounts; Lending activities, particularly loans secured by cash collateral and marketable securities; Non-deposit account services (e.g., nondeposit investment products and insurance). On Customers and Entities, the Manual states that..."Although any type of account is potentially vulnerable to money laundering or terrorist financing, by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific risks. At this stage of the risk assessment process, it is essential that banks exercise judgment and neither define nor treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk, banks should consider other variables, such as services sought and geographic locations." The Manual highlights in particular Customers and Entities posing increased inherent risks As follows: "Foreign financial institutions, including banks and foreign money services providers (e.g., casas de cambio, currency exchanges, and money transmitters). Nonbank financial institutions (e.g., money services businesses; casinos and card clubs; brokers/dealers in securities; and dealers in precious metals, stones, or jewels). Senior foreign political figures and their immediate family members and close associates (collectively known as politically exposed persons (PEP)); Nonresident alien and accounts of foreign individuals; Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies and Private Investment Companies (PIC) and international business corporations (IBC) located in higher-risk geographic locations; Deposit brokers, particularly foreign deposit brokers. Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages); Nongovernmental organisations and charities (foreign and domestic). Professional service providers (e.g., attorneys, accountants, doctors, or real estate brokers). On Geographic Locations, the Manual states that..."Identifying geographic locations that may pose a higher risk is essential to a bank's BSA/AML compliance programme. U.S. banks should understand and evaluate the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a customer's or transaction's risk level, either positively or negatively. Higher-risk geographic locations can be either international or domestic. International higher-risk geographic locations generally include: Countries subject to OFAC sanctions, including state sponsors of terrorism. Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State; Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special

measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act. Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorist financing identified as non-cooperative by international entities such as the Financial Action Task Force on Money Laundering (FATF). Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries which are identified as jurisdictions of primary concern; Offshore financial centers (OFC); Other countries identified by the bank as higher-risk because of its prior experiences or other factors (e.g., legal considerations, or allegations of official corruption); Domestic higher-risk geographic locations may include, but are not limited to, banking offices doing business within, or having customers located within, a U.S. government-designated higher-risk geographic location. The Manual then goes on to explain what should happen next...."the second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess BSA/AML risk. This step involves evaluating data pertaining to the bank's activities (e.g., number of domestic and international funds transfers; private banking customers; foreign correspondent accounts; PTAs; and domestic and international geographic locations of the bank's business area and customer transactions) in relation to Customer Identification Programme (CIP) and customer due diligence (CDD) information. The Manual explains that..."the detailed analysis is important because.....it....gives management a better understanding of the bank's risk profile in order to develop the appropriate policies, procedures, and processes to mitigate the overall risk," and once the risk profile of the firm is understood, management..."should structure the bank's BSA/AML compliance programme to adequately address its risk profile, as identified by the risk assessment,"for example...."the bank's monitoring systems to identify, research, and report suspicious activity should be risk-based, with particular emphasis on higher-risk products, services, customers, entities, and geographic locations as identified by the bank's BSA/AML risk assessment." The Manual also reminds as to the implementation of consolidated or partially consolidated BSA/AML compliance programmes and so recommends that risk assessments should be carried out within business lines and across all activities and legal entities in a consolidated group adopting a consistent methodology..." Aggregating BSA/AML risks on a consolidated basis for larger or more complex organisations may enable an organisation to better identify risks and risk exposures within and across specific lines of business or product categories. Consolidated information also assists senior management and the board of directors in understanding and appropriately mitigating risks across the organisation." As to frequency the Manual states that..."To avoid having an outdated understanding of the BSA/AML risk exposures, the banking organisation should continually reassess its BSA/AML risks and communicate with business units, functions, and legal entities. The identification of a BSA/AML risk or deficiency in one area of business may indicate concerns elsewhere in the organisation, which management should identify and control,"and.... an effective risk assessment should be an ongoing process, not a one-time exercise. Management should update its risk assessment to identify changes in the bank's risk profile, as necessary (e.g., when new products and services are introduced, existing products and services change, higher-risk customers open and close accounts, or the bank expands through mergers and acquisitions). Even in the absence of such changes, it is a sound practice for banks to periodically reassess their BSA/AML risks at least every 12 to 18 months."

3. According to FINTRAC the Canadian FIU an AML Risk Assessment is one of the fundamental components of the risk based approach and critical pillar in designing and implementing an anti-money laundering compliance Programme. In its "Guideline 4: Implementation of a Compliance Regime issued in May 2011 [online] Available at <<http://www.fintrac-canafe.gc.ca/publications/guide/Guide4/4-eng.asp#s661>> [Accessed on 23 July 2013], FINTRAC state that a risk assessment is an analysis of potential threats and vulnerabilities to money laundering and terrorist financing to which your business is exposed.....that the complexity of the assessment depends on the size and risk factors of your business....and....you have to document and consider the following factors in your assessment: your products and services and the delivery channels through which you offer them; the geographic locations where you conduct your activities and the geographic locations of your clients; other relevant factors related to your business; and your clients and the business relationships you have with them." For products, services and delivery channels..."you have to be aware of and recognise products and services or combinations of them that may pose higher risks of money laundering or terrorist financing. Legitimate products and services can be used to mask illegal origins of funds, to move funds to finance terrorist acts or to hide the true identity of the actual owner or beneficiary of the product or service. Products and services that can support the movement and conversion of assets into, through and out of the financial system may pose a high risk. For example, these could include a money laundering related sale of high value goods that resulted in a cheque payable to a bearer which is then deposited into another individual's account to make the transaction difficult to trace and detect. In addition, you may also consider services identified by regulators, governmental authorities or other credible sources as being potentially high risk for

money laundering or terrorist financing. For example, international correspondent banking services, international private banking services, or services involving banknote and precious metal trading and delivery. You have to consider, in a manner that is appropriate to you, the channels used to deliver your products or services. In today's economy and global market, many delivery channels do not bring the client into direct face-to-face contact with you (for example, Internet, telephone or mail), and are accessible 24 hours a day, 7 days a week, from almost anywhere. The more remote a client is from you, the more likely you will have to depend on a third party to deliver your products or services. The remoteness of some of these distribution channels can also be used to obscure the true identity of a client or beneficial owners and can therefore pose higher risks. In addition, you should consider new or innovative services or delivery channels that you may use to deliver your products or services. For geographic locations...."you have to consider, in a manner that is appropriate to you, whether geographic locations in which you operate or undertake activities pose a potentially higher risk for money laundering and terrorist financing. Depending on your business and operations, geographic locations can range from your immediate surroundings, whether rural or urban to a province or territory, multiple jurisdictions within Canada (domestic) or other countries. For example, large entities that operate in a number of domestic jurisdictions may refine the geographic locations factor to differentiate between urban locations having known higher crime rates in comparison to other urban or rural districts. Smaller entities that restrict their activities to a single geographic location or district may not need to make that distinction." For other relevant factors...."you need to consider, in a manner that is appropriate to you, any other factors that are relevant to you, your business or sector. For example, you may offer products or services that can be used to convert funds to a more liquid form, such as electronic wallet, internet payment services or mobile payments. Your business activities may also be more attractive to launder money or fund terrorist activity...and for...Client's and other business relationships...."you have to consider the nature and business of your clients and their relationships with you to determine the level of risk of money laundering and terrorist financing. In other words, you have to know your clients to perform a risk assessment. Knowing your clients is not limited to identification or record keeping requirements. It is about understanding your clients, including their activities, transaction patterns, how they operate and so on. Other elements, such as the magnitude of a client's assets or the number of transactions involved, might also be relevant. Although you should obtain this information through your dealings with the client, it does not necessarily mean that you have to ask the client for additional information or identification documents. You should consider clients you do not know as higher risk than those that you know. Completing a client risk assessment should be appropriate where there is an ongoing relationship. In addition to assessing risk regarding existing clients, for new clients, it is recommended that you perform a risk assessment at the beginning of a client relationship, although a comprehensive risk profile may only become evident once the client has conducted financial transactions with you. However, if you decide to complete a risk rating of new clients, the client identification and information gathering measures at account opening should be robust enough to provide the information needed to feed into your client risk assessment. When assessing a client relationship, consider its duration, the client's number of accounts (if applicable), the products and services used and the client's activities. You may also consider third parties that can be involved in the client's relationship for their impact on the client's risk if you are required to make third party determination. Furthermore, you also have to consider the beneficial owners of an entity for their impact on risk if you are required to obtain this information. Situations where you facilitate a transaction for which a client is acting on behalf of a third party but does not know anything about the third party, may lead you to consider that client as a higher risk. Similarly, a client acting on behalf of an entity who is not aware of the entity's beneficial owners (such as the names of the entity's directors or the individuals controlling the entity for example), may lead you to consider that client as a higher risk. If you know that your client is a politically exposed foreign person (even when you are not required to make the determination or keep related records), you should consider that client as being a higher risk. You should also consider unusual circumstances, cash-intensive businesses and other indicators as potential high risks."

4. For Austrac, the relevant risks for ML/TF are business risk and regulatory risk. "Business risk" is the risk that the business may be used for ML/TF and "Regulatory risk" is associated with not meeting obligations under applicable AML/CTF Regulations." Whilst Austrac do not recommend any one method, and they recognise alternative methods exist and may be appropriate, they have designed and published a methodology for conducting an AML Risk Assessment and a tool to go with it for possible use by businesses though they recognise that reporting entities may choose an alternative method which is appropriate to their business (size, nature and complexity) and the money laundering and/or terrorism financing. The Austrac Methodology for Risk Assessment is made up of four phases; Risk Identification; Risk Assessment; Risk Treatment and Monitoring and Review. Phase 1 is the Risk identification Phase, where the main ML/TF risks and the Regulatory risks are to be identified across the following risk categories: customers; products & services; business practices/delivery methods and with the countries you do business with.

Phase 2 is the Risk assessment/measurement Phase, where the size & importance of the risks identified are measured. Measurement is carried out by considering the likelihood, i.e. the chance of the risk happening and multiplying this by the impact, i.e. the amount of loss or damage if the risk happened. Phase 3 is the Risk Treatment Phase where the intention is to utilise the risk scores obtained to ensure these risks now properly evaluated receive appropriate responses in order to effectively manage and minimize the risks to an acceptable level. Phase 4 is the Monitor and Review Phase in order to keep the methodology and the process and results current. Keeping records and performing a regular evaluation of the risk plan and AML/CTF programme is essential. The risk management plan and AML/CTF programme cannot remain static as risks change over time; for example, changes to the customer base, products and services, business practices and the regulations. Once documented, the methodology and process should be regularly checked and updated. Austrac provide tables and examples of how risk assessments can work. For more details see [online]: Available at <http://www.austrac.gov.au/risk_management.html>. [Accessed 23 July 2013]

5. The UK Joint Money Laundering Steering Group Guidance Notes outlines some of the considerations that should be taken into account when conducting a risk assessment, with taking a risk based approach being a core theme. [online]: Available at: <<http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidancecurrent>>. [Accessed 24 July 2013]

6. This scenario approach seems to be the one favoured by Austrac, the Australian FIU. Austrac believes, "that as "risk" can be defined as the combination of the probability of an event and its consequences or in simple terms risk can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur. "Risk management" is the process of recognising risk and developing methods to both minimise and manage the risk. This requires the development of a method to identify, measure and treat (deal with) risk exposures. This method is the "risk assessment" where the risks are assessed against the likelihood (chance) of them occurring and the severity or amount of loss or damage (impact) which may result if they do happen.

7. Basel Committee on Banking Supervision (2004) [online] 'Revised Framework for the International Convergence of Capital Measurement and Capital Standards', which specified the definitive rules on capital charges for Operational Risk under Basel II (Section 665 Basel 2004); Available at: <http://www.bis.org/publ/bcbs107.htm> [Accessed 8 September 2013]

Part 2, Section 5, Regions, Countries, Criminals and Terrorists

Introduction

1. Forbes. 2012. Joaquin Guzman Loera. Forbes: Powerful People, Dec 2012. [online] Available at: <<http://www.forbes.com/profile/joaquin-guzman-loera/>> [Accessed 19 June 2013]
2. UN's Al-Qaeda Sanctions List 2013. Available at: <http://www.un.org/sc/committees/1267/entities_other-groups_undertakings_associated_with_Al-Qaida.shtml> [Accessed 20 September 2013]
3. UN Office on Drugs and Crime. 2007. Cocaine Trafficking in West Africa: The Threat to Stability and Development. [online] Available at: <http://www.unodc.org/documents/data-and-analysis/west_africa_cocaine_report_2007-12_en.pdfs> [Accessed 19 June 2013]
4. BBC News. 2006. Nigeria oil 'total war' warning. [online] Available at: <<http://news.bbc.co.uk/1/hi/world/africa/4723076.stm>> [Accessed 19 June 2013]
5. National Coalition of Anti-Deportation Campaigns. 2012. Nigeria: Boko Haram targeting schools in North. [online] Available at: <<http://ncadc.org.uk/coi/2012/03/nigeria-boko-haram-targeting-schools-in-north/>> [Accessed 19 June 2013]
6. Lords Resistance Army Crises Tracker [online]: Available at: <<http://www.lracisestracker.com>> [Accessed 20 August 2013].
7. Bloomberg. 2011. Obama sends troops against Uganda rebels. [online] Available at: <<http://www.bloomberg.com/news/2011-10-14/obama-sends-troops-against-uganda-rebels.html>> [Accessed 19 June 2013]
8. BBC News. 2001. Rebels Claim Angolan Train Attack. [online] Available at: <<http://news.bbc.co.uk/1/hi/world/africa/1489317.stm>> [Accessed 19 June 2013]
9. Abe Selig. 2008. Alperon's Son: I'll cut off killer's arms and legs. Jerusalem Post 18 November 2008. [online] Available at: <<http://www.jpost.com/Israel/Alperons-son-Ill-cut-off-killers-arms-and-legs>> [Accessed 19 June 2013]
10. Wikipedia, the free Encyclopaedia. 2013. Zeev Rosenstein. [online] Available at: <http://en.wikipedia.org/wiki/Zeev_Rosenstein> [Accessed 19 June 2013]
11. BBC: On This Day. 1985: Gunmen kill 18 at two European Airports. [online] Available at: <http://news.bbc.co.uk/onthisday/hi/dates/stories/december/27/newsid_2545000/2545949.stm> [Accessed 19 June 2013]
12. US Department of State. 2004. Zarqawi Letter. [online] Available at: <<http://www.au.af.mil/au/awc/awcgate/>>

- state/31694.htm> [Accessed 19 June 2013]
13. Council on Foreign Relations. 2012. Al-Qaeda in the Arabian Peninsula (AQAP). [online] Available at <<http://www.cfr.org/yemen/al-qaeda-arabian-peninsula-aqap/p9369>> [Accessed 19 June 2013]
 14. Turkish Counter Terrorism and Operations Department of Directorate General for Security: Available at <http://en.wikipedia.org/wiki/List_of_illegal_political_parties_in_Turkey> [Accessed 20 September 2013]
 15. Jongerden, J., and Akkaya, A. H. 2012. The Kurdish Workers Party and a New Left in Turkey: Analysis of the revolutionary movement in Turkey through the PKK's memorial text on Haki Karer. European Journal of Turkish Studies vol 14. [online] Available at: <<http://ejts.revues.org/4613>> [Accessed 19 June 2013]
 16. Preston, J. 2005. Afghan Arrested in New York said to be a Heroin Kingpin. The New York Times, April 26 2005. [online] Available at: <http://www.nytimes.com/2005/04/26/international/asia/26afghan.html?_r=0> [Accessed 19 June 2013]
 17. CBC News. 2011. Pakistan Taliban claim bombings that kill 80. CBC News: World 12 May 2011. [online] Available at: <<http://www.cbc.ca/news/world/story/2011/05/12/pakistan-bombing.html>> [Accessed 19 June 2013]
 18. BBC News. 2006. Nepal peace breakthrough welcomed. [online] Available at: <http://news.bbc.co.uk/1/hi/world/south_asia/6128062.stm> [Accessed 19 June 2013]
 19. Constitution of the Democratic Socialist Republic of Sri Lanka: Chapter II: Buddhism. 2000. [online] Available at: <<http://www.commonlii.org/lk/legis/const/2000/3.html>> [Accessed 19 June 2013]
 20. The Independent. 2009. Tamil Tigers: defeated at home, defiant abroad. [online] Available at: <<http://www.independent.co.uk/news/uk/home-news/tamil-tigers-defeated--at-home-defiant-abroad-1689766.html>> [Accessed 19 June 2013]
 21. China Ministry of Public Security (2003) Available at <http://news.xinhuanet.com/english/2003-12/15/content_1231167.htm> [Accessed 20 September 2013]
 22. Australian Govt; Australian National Security (2013) (online) Available at: <http://www.nationalsecurity.gov.au/agd/WWW/NationalSecurity.nsf/Page/What_Governments_are_doingListing_of_Terrorism_>Organisations> [Accessed 12 September 20103]
 23. US Department of State 2013 [online] Available at: <<http://www.state.gov/j/ct/rls/other/des/123085.htm>> [Accessed 20 September 2013]
 24. US Department of State 2013 [online] Available at: <<http://www.state.gov/j/ct/rls/other/des/123086.htm>> [Accessed 20 September 2013]The Terrorist Exclusion List Designees are as follows (alphabetical listing): Afghan Support Committee; Al Taqwa Trade; Al-Hamati Sweets Bakeries; Al-Irtithad al-Islami (AIAI); Al-Manar; Al-Ma'unah; Al-Nur Honey Center; Al-Rashid Trust; Al-Shifa Honey Press for Industry and Commerce; Al-Wafa al-Igatha al-Islamia (a.k.a. Wafa Humanitarian Organisation); Alex Boncayaao Brigade (ABB); Anarchist Faction for Overthrow; Army for the Liberation of Rwanda (ALIR) (a.k.a. Interahamwe, Former Armed Forces (EX-FAR)); Asbat al-Ansar; Babbar Khalsa International; Bank; Black Star; Continuity Irish Republican Army (CIRA); Darkazanli Company; Dhamat Houmet Daawa Salafia (a.k.a. Group; Protectors of Salafist Preaching; a.k.a. Houmat Ed Daawa Es Salifiya); a.k.a. Katibat El Ahoual; a.k.a. Protectors of the Salafist Predication; a.k.a. El-Ahoual Battalion; a.k.a. Katibat El Ahouel; a.k.a. Houmat Ed-Daawa Es-Salafia; a.k.a. the Horror Squadron; a.k.a. Djamaat Houmat Eddawa Essalafia; a.k.a. Djamaatt Houmat Ed Daawa Es Salafiya; a.k.a. Salafist Call Protectors; a.k.a. Djamaat Houmat Ed Daaqua es-Salafia; a.k.a. Group of Supporters of the Salafiste Trend; a.k.a. Group of Supporters of the Salafist Trend; Eastern Turkistan Islamic Movement; First of October Antifascist Resistance Group (GRAPO) (a.k.a. Grupo de Resistencia Anti-Fascista Premier De Octubre); Harakat ul Jihad i Islami (HUIJ); International Sikh Youth Federation; Islamic Army of Aden; Islamic Renewal and Reform Organisation; Jamiat al-Ta'awun al-Islamiyya; Jamiat ul-Mujahideen (JUM); Japanese Red Army (JRA); Jaysh-e-Mohammed; Jayshullah; Jerusalem Warriors; Lashkar-e-Tayyiba (LET) (a.k.a. Army of the Righteous); Libyan Islamic Fighting Group; Loyalist Volunteer Force (LVF); Makhtab al-Khidmat; Moroccan Islamic Combatant Group; Nada Management Organisation (f.k.a. Al Taqwa Management Organisation SA); New People's Army (NPA); Orange Volunteers (OV); People Against Gangsterism and Drugs (PAGAD); Red Brigades-Combatant Communist Party (BR-PCC); Red Hand Defenders (RHD); Revival of Islamic Heritage Society (Pakistan and Afghanistan offices); Revolutionary Proletarian Nucleus; Revolutionary United Front (RUF); Salafist Group for Call and Combat (GSPC); The Allied Democratic Forces (ADF); Islamic International Peacekeeping Brigade; The Lord's Resistance Army (LRA); The Pentagon Gang; The Riyadus-Salikhin Reconnaissance and Sabotage; Tunisian Combat Group; Turkish Hezbollah; Ulster Defense Association (a.k.a. Ulster Freedom Fighters); Ummah Tameer E-Nau (UTN); Youssef M. Nada & Co. Gesellschaft M.B.H. Groups Delisted from the Terrorist Exclusion List (alphabetical listing) are the Communist Party of Nepal (Maoist) (a.k.a. CPN(M)); a.k.a. the United Revolutionary People's Council, a.k.a. the People's Liberation Army of

- Nepal)
25. Richardson, J. H. 1997. The Latin Kings Play Songs of Love. New York Magazine, Feb 1997. pp 28-37
 26. The Federal Bureau of Investigation. FBI Records: The Vault: Aryan Brotherhood. [online] Available at: <<http://vault.fbi.gov/Aryan%20Brotherhood%20/Aryan%20Brotherhood%20Part%201%20of%201/view>> [Accessed 19 June 2013]
 27. US Department of Justice. 2013. Motorcycle Gangs. [online] Available at: <<http://www.justice.gov/criminal/ocgs/gangs/motorcycle.html>> [Accessed 19 June 2013]
 28. Source: Canadian Government: Public Safety Canada <http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntns/crrnt-lstd-ntns-eng.aspx>
 29. The Drug War in Mexico, US Mexico Security Challenges 2013: Trans Border Institute; Joan B Kroc School of Peace Studies; University of San Diego: 2013 (online): Available at: <<http://catcher.sandiego.edu/items/peacestudies/Shirk-Mexico%20Security-sm.pdf>> [Accessed on 30 September 2013]"
 30. Carlyle, E. 2012. "El Chapo" Named "World's Most Powerful Drug Trafficker". Forbes Dec 2012. [online] Available at: <<http://www.forbes.com/sites/erincarlyle/2012/01/11/el-chapo-named-worlds-most-powerful-drug-trafficker/>> [Accessed 19 June 2013]
 31. Associated Press. 2010. Calderon: Mexico Drug Gangs Seeking to Replace Government. Huffington Post. [online] Available at: <http://www.huffingtonpost.com/2010/08/05/calderon-mexico-drug-gang_n_671555.html> [Accessed 19 June 2013]
 32. Landler, M. 2009. Clinton Says US Feeds Mexico Drug Trade. The New York Times. [online] Available at: <http://www.nytimes.com/2009/03/26/world/americas/26mexico.html?_r=0> [Accessed 19 June 2013]
 33. In a draft paper for a National Defense University journal, former Washington Post reporter and International Assessment and Strategy Center (IASC) fellow Douglas Farah argues that Mexican transnational criminal organisations (TCOs) have consolidated in Guatemala, Honduras, and El Salvador, also known as the Northern Triangle, to the extent that they have become the de facto authority, making the state "almost non-functional." In Farah's view, this has the potential to turn the Northern Triangle countries into criminal, rather than simply weak, states. His key points include: 1. Real power now rests with the TCOs and their allies. Mexican criminal groups have co-opted already weak government structures in the three countries through contacts in corrupt security, justice and government bodies. This in turn has paved the way for the entry of other TCOs such as Colombian guerrillas from the FARC, the Spanish separatist group ETA, and even Hezbollah. "There are virtually no 'ungoverned spaces' in the region," Farah writes. "What has changed is that the authority is less and less often the state." This is reflected in decreasing state resources and accessible to citizens, as well as citizen perceptions of state incompetence, Farah states. In contrast with the transport groups that existed in the Northern Triangle prior to the infiltration of Mexican criminal groups, the TCOs work to control territory, which they use to set up power bases and front businesses, including private security firms. According to Farah, territorial control is a key element of TCO power consolidation, allowing them to fulfill functions traditionally associated with the state. He notes that this is less true in El Salvador, where the street gangs, or "maras," not the TCOs, have the most power. 2. The states themselves have allowed this power shift to happen. "The state itself at times becomes a part of the criminal enterprise," writes Farah, adding that Central America's Northern Triangle is particularly attractive to criminal groups because TCOs are drawn to weak rather than failed states. While a failed state may have no real institutional structure to work with, weak state institutions provide the opportunity to co-opt security bodies, law enforcement officials, judicial officials, and politicians.. Criminals work with the state through what Farah calls a "transactional paradigm" -- for example, police perform executions in exchange for money. According to Farah, this paradigm helps to explain "anomalies" present in these states, such as the persistence of extremely high homicide rates despite extremely high levels of incarceration. 3. The US sees the risk, but is taking inappropriate measures. The US recognises that it will be affected by a loss of rule of law in Central America, not least because of the large amount of US-bound cocaine flowing through the region. However, the US has continued to funnel money into anti-drug efforts in these corrupt, weak states, which are unable or unwilling to effectively use these funds, Farah says. The US also lacks trustworthy public officials with whom to build relationships in these countries. Farah notes that the US has helped directly contribute to the problem, deporting thousands of gang members back to these already weak and overburdened states. Meanwhile, Mexico and other Central American governments have increasingly shifted their focus to violence reduction over anti-drug efforts, a strategy which is arguably based on the assumption that large-scale criminal structures will always exist. The US has also shifted policy somewhat, focusing more on economic and trade issues in the region.
 34. The CFZ serves as a transhipment point for some goods bought with drugs proceeds .This is often dollars obtained in the US and through Colombian Black Market Peso Exchange mechanisms. According to the CFZ's own website it has over 2,600 business, 25 bank branches, and employs approximately 25,000 personnel. Moving

Counterfeit goods is another, often compounding, problem in the Free Zone. The ports of Panama handle over 4 million twenty-foot equivalent units (TEUs) of container traffic per year.

35. Council on Foreign Relations. 2006. Brazil's Powerful Prison Gang. [online] Available at: <<http://www.cfr.org/brazil/brazils-powerful-prison-gang/p11542>> [Accessed 19 June 2013]
36. According to the Peruvian government, drug trafficking accounted for almost 17% of GDP in 2009. Environmental Campaigners are also concerned about the damage coca growing and cocaine production is having on the rainforests, both because of deforestation and the dumping of the chemicals involved in the drug's manufacture. Cocaine is transported over land to neighbouring countries, and onwards to Europe, the Far East, Mexico, the Caribbean, and the US using a variety of ships and commercial air flights. Maritime smuggling is the primary method for transporting multi-ton loads of cocaine. Colombians and Mexicans operate drug transportation networks in Peru, shipping cocaine to Colombia, Mexico, and the Caribbean mainly using seaborne smuggling US law enforcement agencies and their counterparts in Australia, Hong Kong, Japan, Malaysia, and Thailand have also reported that cocaine trafficking and transportation organisations from Peru operate in the Far East. Peru is also a major importer of the precursor chemicals used for cocaine production. Peru is not regarded as a major regional financial centre Peru's financial intelligence unit (Unidad de Inteligencia Financiera del Perú F.U.) has estimated that approximately US\$3billion of illegal proceeds passes through Peruvian financial organisations each year, accounting for approximately 2% of Peru's GDP. Drug trafficking and related businesses account for 84% of this amount and the remaining relates to tax fraud, corruption, and illegal arms trading. As a consequence large scale laundering occurs that includes casinos, property sales, business investments, construction, export businesses, hotels, and restaurants. Peru's economy is very cash-based with a heavy use of the US dollar in a large informal sector. Pervasive corruption, informal money exchange and wire transfer services also encourage money laundering. Gambling is also highly susceptible to money laundering and there are no restrictions on cash-to-cash, cash-to-cheque, or cash-to-wire transfer transactions in casinos. It is estimated that currently 700 establishments are licensed. Like other states in the region there is a black market for pirated and smuggled goods in which cash transactions are the norm. Corruption is a major problem in Peru with the Government estimating that the budget loses 15% per year due to corruption. Peru is a source of, and destination for labour and sex trafficking with several thousand persons, mainly male are estimated to be subjected to conditions of forced labour within Peru, mainly in mining, logging, agriculture, and domestic service. Women and girls are recruited and forced into prostitution in the clubs, bars, and brothels of the country's cities and mining centres. . Peruvian women are also, to a lesser extent, forced into prostitution in Ecuador, Spain, Italy, Japan, and the US, and forced labour in neighbouring states. Indigenous persons are particularly vulnerable to debt bondage. Forced child labour is a problem, particularly in informal gold mines. Child sex tourism is present in Cuzco and Lima. Peru also is a destination country for some Ecuadorian, Bolivian, and Chinese women and girls subjected to sex trafficking.
37. InSight Crime. 2013. Walid Makled. [online] Available at: <<http://www.insightcrime.org/personalities-venezuela/walid-makleds>> [Accessed 19 June 2013]
38. For details on Russian Oligarchs see Note 7 in Part 1, Section 1, Money Laundering Crimes; Bribery and Corruption above
39. Official Journal of the European Union 2013 [online] Available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:165:0072:01:EN:HTML>> [Accessed 20 September 2013]
40. Terrorist Organisations Designated by France: Available at: <http://www.start.umd.edu/start/data_collections/tops/terrorist_organizations_by_country.asp?id=FR> [Accessed 20 September 2013]
41. UK Government (2013) (online) Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/232176>List_of_Proscribed_organisations.pdf>

Part 2, Section 6 - Terrorist Attacks

Introduction and Chronology of the World's Worst Terrorist Attacks Over the Last 100 Years and World's Worst Airline Attacks by Terrorists

1. Maplecroft: Global Risk Analytics. 2011. Newly formed South Sudan joins Somalia, Pakistan, Iraq and Afghanistan at top of Maplecroft terrorism ranking – attacks up 15% globally. [online] Available at: <http://maplecroft.com/about/news/terrorism_index_2011.html> [Accessed 21 June 2013]
2. BBC: On This Day (21, 1974). 2013. 1974: Birmingham pub blasts remembered. [online] Available at: <http://news.bbc.co.uk/onthisday/hi/witness/november/21/newsid_4025000/4025491.stm> [Accessed 21 June 2013]
3. BBC: On This Day (27, 1979). 2013. 1979: IRA bomb kills Lord Mountbatten. [online] Available at: <http://news.bbc.co.uk/onthisday/hi/dates/stories/august/27/newsid_2511000/2511545.stm> [Accessed 21 June 2013]

Part 2, Section 7 - Criminal Cases

1. "events, dear boy, events" – the response given by British Prime Minister Harold Macmillan to the question posed by a journalist when asked what is most likely to blow governments off-course though the existence even of the quote itself is disputed and largely attributed.
2. Block, M. 2006. The 'Rumsfeld Rules' of Public Discourse. [online] Available at: <<http://www.npr.org/templates/story/story.php?storyId=6457639>> [Accessed 27 June 2013]
3. 1999. Prepared Remarks of Amy G Elliott Delivered to the US Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs. [online] Available at: <<http://www.hsgac.senate.gov/download/?id=5374edfe-248e-4855-be83-ccf3a749b039>> [Accessed 27 June 2013]
4. London School of Economics. 2011. 'Howard Davies statement – stepping down'. [online] Available at: <<http://www.lse.ac.uk/newsAndMedia/woolf/howardSteppingDown.aspx>> [Accessed 27 June 2013]
5. US Securities and Exchange Commission. 2006. 'SEC Sanctions Statoil for Bribes to Iranian Government Official'. [online] Available at: <<http://www.sec.gov/news/press/2006/2006-174.htm>> [Accessed 27 June 2013]
6. US Securities and Exchange Commission. 2009. SEC Charges KBR and Halliburton for FCPA Violations. [online] Available at: <<http://www.sec.gov/news/press/2009/2009-23.htm>> [Accessed 27 June 2013]
7. Neville, S. 2012. 'GlaxoSmithKline fined \$3bn after bribing doctors to increase drugs sales' The Guardian Online. [online] Available at: <<http://www.guardian.co.uk/business/2012/jul/03/glaxosmithkline-fined-bribing-doctors-pharmaceuticals>> [Accessed 27 June 2013]
8. McLean, B. 2006. 'Is Enron Overpriced?' Fortune Online. [online] Available at: <http://money.cnn.com/2006/01/13/news/companies/enronoriginal_fortune/> [Accessed 27 June 2013]
9. Berenson, A., Oppel, R. A. 2001. 'Enron's Chief Executive Quits After Only 6 Months in Job' The New York Times. [online] Available at: <<http://www.nytimes.com/2001/08/15/business/enron-s-chief-executive-quits-after-only-6-months-in-job.html>> [Accessed 27 June 2013]
10. Dizikes, P. 2013. 'Enron Worker Warned Lay of Accounting Scandals' ABC News. [online] Available at: <<http://abcnews.go.com/Business/story?id=87418&page=1#.UcxSYNiLWNs>> [Accessed 27 June 2013]
11. Elkind, P., McLean, B. 2003. 'The Smartest Guys in the Room: The Amazing Rise and Scandalous Fall of Enron' QFinance. [online] Available at: <<http://www.qfinance.com/business-ethics-finance-library/the-smartest-guys-in-the-room-the-amazing-rise-and-scandalous-fall-of-enron>> [Accessed 27 June 2013]
12. US Congress. 2002. 'Sarbanes-Oxley Act of 2002'. [online] Available at: <<http://taft.law.uc.edu/CCL/SOact/soact.pdf>> [Accessed 27 June 2013]
13. US Government Printing Office. 2003. 'Fishtail, Bacchus, Sundance, and Slapshot: Four Enron Transactions Funded and Facilitated by US Financial Institutions'. [online] Available at: <<http://www.gpo.gov/fdsys/pkg/CPRT-107SPRT83559/html/CPRT-107SPRT83559.htm>> [Accessed 27 June 2013]
14. Beresford, D., de Katzenbach, N., Rogers Jr., C. B. 2003. 'Report of Investigation by the Special Investigative Committee of the Board of Directors of Worldcom, Inc.' [online] Available at: <<http://www.sec.gov/Archives/edgar/data/723527/000093176303001862/dex991.htm>> [Accessed 27 June 2013]
15. Febureau. 2009. 'It was like riding a tiger, not knowing how to get off without being eaten' The Financial Express. [online] Available at: <<http://www.financialexpress.com/news/it-was-like-riding-a-tiger-not-knowing-how-to-get-off-without-being-eaten/407917>> [Accessed 27 June 2013]
16. US Securities and Exchange Commission. 2006. In the Matter of Samuel Israel III and Daniel E. Marino, Exchange Act Rel. No. 53775 / May 9, 2006. [online] Available at: <<http://www.sec.gov/litigation/litreleases/2006/lr19692.htm>> [Accessed 27 June 2013]
17. David Kotz, H. 2010. Report of Investigation of Failure of the SEC to Uncover Bernard Madoff's Ponzi Scheme. DIANE publishing.
18. BBC News. 2009. 'Kreuger: The original Bernard Madoff?' [online] Available at: <<http://news.bbc.co.uk/1/hi/business/7939403.stm>> [Accessed 27 June 2013]
19. Truell, P. 1995. 'A Japanese Bank Is Indicted In US and Also Barred' The New York Times [online] Available at: <<http://www.nytimes.com/1995/11/03/business/a-japanese-bank-is-indicted-in-us-and-also-barred.html?pagewanted=all&src=pm>> [Accessed 28 June 2013]
20. BBC News. 2000. 'Bank bosses pay \$775m fraud charge'. [online] Available at: <<http://news.bbc.co.uk/1/hi/business/933834.stm>> [Accessed 28 June 2013]
21. The Independent. 1996. 'How 'Mr Copper' became the world's biggest fraud' The Independent Online. [online] Available at: <<http://www.independent.co.uk/news/how-mr-copper-became-the-worlds-biggest-fraud-1337059.html>> [Accessed 28 June 2013]
22. US Securities and Exchange Commission. 2004. In the Matter of Orlando Joseph Jett. [online] Available at:

- <<http://www.sec.gov/litigation/opinions/33-8395.htm>> [Accessed 28 June 2013]
23. Nasar, S. 1994. 'Behind the Kidder Scandal: The Overview; Kidder Scandal Tied to Failure of Supervision' The New York Times. [online] Available at: <<http://www.nytimes.com/1994/08/05/us/behind-kidder-scandal-overview-kidder-scandal-tied-failure-supervision.html?pagewanted=all&src=pm>> [Accessed 28 June 2013]
24. Trichur, R. 2009. 'Optional 'plied' former traders with gifts: BMO' The Toronto Star [online] Available at: <http://www.thestar.com/business/2009/09/02/optional_plied_former_traders_with_gifts_bmo.html> [Accessed 28 June 2013]
25. Hough, A., Rayner, R., Ward, V. 2011. 'I need a miracle: rogue trader Kweku Adoboli who lost UBS £1.3bn' The Telegraph. [online] Available at: <<http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/8767089/I-need-a-miracle-rogue-trader-Kweku-Adoboli-who-lost-UBS-1.3.bn.html>> [Accessed 28 June 2013]
26. The International Bar Association. 2011. The Khodorkovsky Trial: a report on the observation of the criminal trial of Mikhail Borisovich khodorkovsky and Platon Leonidovich Lebedev, March 2009 to December 2010. [online] Available at: <<http://www.ibanet.org/Document/Default.aspx?DocumentUid=A73BA389-7E3D-4B71-9F68-D4E4455DDA31>> [Accessed 28 June 2013]
27. The Guardian. 2010. 'US Embassy cables: 'Politically motivated' Khodorkovsky trial 'given rule of law gloss' The Guardian Online [online] Available at: <<http://www.guardian.co.uk/world/us-embassy-cables-documents/242087>> [Accessed 28 June 2013]
28. Council of Europe. 2009. Parliamentary Assembly: Allegations of politically motivated abuses of the criminal justice system in Council of Europe member states. [online] Available at: <<http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=12748&Language=EN>> [Accessed 28 June 2013]
29. Khodorkovsky and Lebedev Communications Centre. 2012. [online] Available at: <<http://archive.is/3DQk>> [Accessed 28 June 2013]
30. Jopson, B. 2006. 'Regulator spells it out for Jabre' Financial Times. [online] Available at: <<http://www.ft.com/ms/s/0/cee4431c-1dd4-11db-bf06-0000779e2340.html#axzz2XVeumlo1>> [Accessed 28 June 2013]
31. Federal Bureau of Investigation: Press Release. June 20, 2011. 'Expert-Networking Firm Consultant Found Guilty in Manhattan Federal Court of Insider Trading Crimes' [online] Available at: <<http://www.fbi.gov/newyork/press-releases/2011/expert-networking-firm-consultant-found-guilty-in-manhattan-federal-court-of-insider-trading-crimes>> [Accessed 28 June 2013]
32. Catholic News Agency. 2008. Rosary plays an important role in hostage rescue in Colombia. [online] Available at: <http://www.catholicnewsgroup.com/news/rosary_plays_important_role_in_hostage_rescue_in_colombia/> [Accessed 28 June 2013]
33. Radio France Internationale. 2008. 'Betancourt Speaks to RFI' Radio France Internationale. [online] Available at: <http://www.rfi.fr/actuen/articles/103/article_908.asp> [Accessed 28 June 2013]
34. Federal Energy Regulatory Commission. 2003. Staff Report: Price Manipulation in Western Markets. [online] Available at: <<http://www.ferc.gov/industries/electric/indus-act/wec/enron/summary-findings.pdf>> [Accessed 28 June 2013]
35. US District Court: Southern District of New York. 2008. US Commodity Futures Trading Commission. [online] Available at: <<http://www.cftc.gov/ucm/groups/public/@lrenforcementactions/documents/legalpleading/enfwelshcomplaint031412.pdf>> [Accessed 28 June 2013]
36. Prince, R. 2012. 'Merchant of Death' Viktor Bout sentenced to 25 years in prison' The Telegraph. [online] Available at: <<http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9189852/Merchant-of-Death-Viktor-Bout-sentenced-to-25-years-in-prison.html>> [Accessed 28 June 2013]
37. US Department of Justice. [Press release] 'Federal Jury in Dallas convicts Holy Land Foundation and its leaders for providing material support to Hamas terrorist organisation.' [online] Available at: <http://www.justice.gov/usa/txn/PressRel08/HLF_convict_pr.html> [Accessed 28 June 2013]
38. US Department of the Treasury. 2003. [Press release] 'US Designates Five Charities Funding Hamas and Six Senior Hamas Leaders as Terrorist Entities'. [online] Available at: <<http://www.treasury.gov/press-center/press-releases/Pages/j672.aspx>> [Accessed 28 June 2013]
39. Silver, V. 2005. 'US Muslim Activist Broke Libya Sanctions, Aided Murder Plot' Bloomberg. [online] Available at: <<http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a2JrpSUGcwsc>> [Accessed 28 June 2013]
40. Press Release: Manhatten District Attorney [online]. Available at: <http://manhattanda.org/press-release/district-attorney-morgenthau-announces_indictment_chinese_citizen_fraudulent_business>

Part 2, Section 8 - Enforcement Cases

1. Wikipedia, Nugan Hand Bank, [online] [2013], Available at: http://en.wikipedia.org/wiki/Nugan_Hand_Bank [Accessed 29 May 13]
2. Wikipedia, Branco Ambrosiano, Roberto Calvi, [online] [2013], Available at: http://en.wikipedia.org/wiki/Banco_Ambrosiano [Accessed 29 May 13]
3. Labaton, S. (1988). Drexel Burnham Charged by SEC with Stock Fraud, The New York Times [online]. Available at: <http://www.nytimes.com/1988/09/08/business/drexel-burnham-charged-by-sec-with-stock-fraud.html?pagewanted=all&src=pm> [Accessed 29 May 13]
4. Senate Foreign Relations Committee, A Report to the Committee on Foreign Relations US Senate by Senator John Kerry and Senator Hank Brown; December 1992, [online], Available at: http://www.fas.org/irp/congress/1992_rpt/bcci/ [Accessed 29 May 13]
5. Johnston, D. (1991). BCCI Agrees to Plead Guilty And Will Forfeit \$550 Million, The New York Times [online]. Available: <http://www.nytimes.com/1991/12/20/business/bcci-agrees-to-plead-guilty-and-will-forfeit-550-million.html> [Accessed 29 May 13]
6. BBC News (2005) [online], BCCI liquidators drop £1bn case, Available at: <http://news.bbc.co.uk/2/hi/business/4399336.stm> [Accessed 29 May 13]
7. US Department of Justice (1992) [online], Department of Justice and SEC Enter \$290 Million Settlement with Salomon Brothers in Treasury Security Case, Available at: http://www.justice.gov/atr/public/press_releases/1992/211182.htm [Accessed 29 May 13]
8. Barings Bank: Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings (1995) [online] Available at: <http://www.numa.com/ref/barings/bar00.htm> [Accessed 8 September 2013]
9. Criminal Compliance and Indictment Against Daiwa Bank (1995) [online], The 'Leclerc Law Library. Available at: <http://www.leclerc.law/files/cas60.htm> [Accessed 29 May 13]
10. Truell, P. (1996), Daiwa Bank Admits Guilt in Cover-Up, The New York Times [online]. Available at: <http://www.nytimes.com/1996/02/29/business/daiwa-bank-admits-guilt-in-cover-up.html> [Accessed 29 May 13]
11. Stevenson, T. (1997). Morgan Grenfell fined record pounds 2m over Young, The Independent [online]. Available at: <http://www.independent.co.uk/news/business/morgan-grenfell-fined-record-pounds-2m-over-young-1267655.html> [Accessed 30 May 13]
12. Financial Regulatory Briefing (2000) [online], SFA Disciplines NatWest and 2 Individuals, Available at: http://www.frb.co.uk/cgi-bin/dmr5?access=&runprog=frb/frb_pages&mode=disp&fragment=2000_06_099 [Accessed 30 May 13]
13. Treanor, J. (2000), NatWest fined for options scandal, The Guardian [online]. Available at: <http://www.guardian.co.uk/money/2000/may/19/business.personalfinancenews1> [Accessed 30 May 13]
14. Commodity and Futures Commission (1998) [online], CFTC Files and Settles Actions Against Sumitomo Corporation for Manipulating the Copper Market in 1995-96, Available at: <http://www.cftc.gov/opa/enf98/opa4144-98.htm> [Accessed 30 May 13]
15. Worth, R. (2002), Bank Failed to Question Huge Deposits, The New York Times [online]. Available at: <http://www.nytimes.com/2002/11/28/business/bank-failed-to-question-huge-deposits.html> [Accessed 29 May 13]
16. Boyd, D. (2003), Precedent set with recent drug money laundering cases, US Customs Today [online]. Available at: http://www.cbp.gov/xp/CustomsToday/2003/January/money_laundering.xml [Accessed 29 May 13]
17. US Securities and Exchange Commission (2003), SEC Fact Sheet on Global Analyst Research Settlements [online]. Available at: <http://www.sec.gov/news/speech/factsheet.htm> [Accessed 29 May 13]
18. NY State Office of the Attorney General (2003) [online], New York Signs Historic Agreements With the Nation's Leading Brokerage Firms, Available at: <http://www.ag.ny.gov/press-release/new-york-signs-historic-agreements-nations-leading-brokerage-firms> [Accessed 29 May 13]
19. NY State Office of the Attorney General (2003) [online], State Investigation Reveals Mutual Fund Fraud, Available at: <http://www.ag.ny.gov/press-release/state-investigation-reveals-mutual-fund-fraud> [Accessed 29 May 13]
- Links to individual cases: Theodore C. Sihpol III (Bank of America) (2003) [online], Available at: <http://www.ag.ny.gov/press-release/attorney-general-spitzer-and-securities-and-exchange-commission-file-charges-against> [Accessed 30 May 13]; Steven B. Markovitz (Millennium Partners) (2003) [online], Available at: <http://www.ag.ny.gov/press-release/new-york-attorney-general-and-securities-and-exchange-commission-bring-criminal-and> [Accessed 30 May 13]; James P. Connelly, Jr. (Fred Alger & Co) (2003) [online], Available at: <http://www.ag.ny.gov/press-release/new-york-ag-and-sec-bring-criminal-and-civil-actions-against-mutual-fund-executive> [Accessed 30 May 13]; Pilgrim Baxter (2003) [online], Available at: <http://www.ag.ny.gov/press-release/pbhg-founders-firm-named-fund-timing-suit> [Accessed 30 May 13], Invesco (2003) [online], Available at: <http://www.ag.ny.gov/press-release/invesco> [Accessed 30 May 13]

documents-show-secret-market-timing-arrangements [Accessed 30 May 13]; Alliance Capital Settlement (2003) [online], Available at: <http://www.ag.ny.gov/press-release/statement-attorney-general-eliot-spitzer-regarding-mutual-fund-fee-reduction> [Accessed 30 May 13]; Paul A. Flynn (Canadian Imperial Holdings) (2004) [online], Available at: <http://www.ag.ny.gov/press-release/banker-charged-late-trading> [Accessed 30 May 13]; Massachusetts Financial Services Co. (MFS) Settlement (2004) [online], Available at: <http://www.ag.ny.gov/press-release/mfs-settles-market-timing-issues> [Accessed 30 May 13]; Columbia Management Advisors and Columbia Funds Distributor (subs of FleetBoston) (2004) [online], Available at: <http://www.ag.ny.gov/press-release/spitzer-files-civil-charges-against-fleetboston-subsidiaries-market-timing-case> [Accessed 30 May 13]; Bank of America and FleetBoston Settlement (2004) [online], Available at: <http://www.ag.ny.gov/press-release/spitzer-sec-reach-largest-mutual-fund-settlement-ever> [Accessed 30 May 13]; Sihpol Indictment (2004) [online], Available at: <http://www.ag.ny.gov/press-release/sihpol-indicted-forty-counts-stemming-his-transactions-banc-america> [Accessed 30 May 13]; Janus Capital Settlement (2004) [online], Available at: <http://www.ag.ny.gov/press-release/spitzer-salazar-announce-market-timing-settlement-janus-capital-management-llc> [Accessed 30 May 13]; Strong Capital Settlement (2004) [online], Available at: <http://www.ag.ny.gov/press-release/new-york-wisconsin-settle-market-timing-allegations-strong-capital-management-and-its> [Accessed 30 May 13]; Pilgrim Baxter Settlement (2004) [online], Available at: <http://www.ag.ny.gov/press-release/pilgrim-baxter-settles-market-timing-case> [Accessed 30 May 13]; BancOne Settlement (2004) [online], Available at: <http://www.ag.ny.gov/press-release/spitzer-announces-market-timing-settlement-banc-one-investment-advisors-corporation> [Accessed 30 May 13]; Invesco and AIM Settlements (2004) [online], Available at: <http://www.ag.ny.gov/press-release/invesco-and-aim-settle-mutual-fund-timing-cases> [Accessed 30 May 13]; RS Investments Settlement (2004) [online], Available at: <http://www.ag.ny.gov/press-release/robertson-stevens-settles-market-timing-case> [Accessed 30 May 13]; Fremont Investment Advisors (FIA) Settlement (2004) [online], Available at: <http://www.ag.ny.gov/press-release/fremont-investment-advisors-settles-market-timing-case> [Accessed 30 May 13]; Pilgrim Baxter Settlement (2004) [online], Available at: <http://www.ag.ny.gov/press-release/founders-phbg-funds-settle-market-timing-case> [Accessed 30 May 13]; Scott A. Christian (Trautman Wasserman) (2005) [online], Available at: <http://www.ag.ny.gov/press-release/broker-pleads-guilty-late-trading> [Accessed 30 May 13]; CIBC Settlement: <http://www.ag.ny.gov/press-release/cibc-settles-market-timing-investigation> [Accessed 30 May 13] J. & W. Seligman & Company (2005) [online], Available at: <http://www.ag.ny.gov/press-release/secret-mutual-fund-timing-arrangements-exposed-seligman> [Accessed 30 May 13]; Federated Investors, Inc. Settlement (2005) [online], Available at: <http://www.ag.ny.gov/press-release/federated-settles-mutual-fund-timing-investigation> [Accessed 30 May 13]; Millennium Partners Agreement (2005) [online], Available at: <http://www.ag.ny.gov/press-release/mutual-fund-timing-fraud-revealed-millennium-partners> [Accessed 30 May 13]; Prudential Equity Group Settlement (2006) [online], Available at: <http://www.ag.ny.gov/press-release/prudential-settles-market-timing-investigations> [Accessed 30 May 13]; Fred Alger Management, Inc. Settlement (2006) [online], Available at: <http://www.ag.ny.gov/press-release/alger-settles-market-timing-case-45-million> [Accessed 30 May 13]; Related US Securities and Exchange Commission Settlements and Actions (2004) [online], Available at: <http://www.sec.gov/news/press/pressarchive/2004press.shtml>; (2005) [online], Available at: <http://www.sec.gov/news/press/pressarchive/2005press.shtml>; (2006) [online], Available at: <http://www.sec.gov/news/press/pressarchive/2006press.shtml>; Christian (Trautman Wasserman) (2005) [online], Available at: <http://www.sec.gov/litigation/complaints/comp19294.pdf> [Accessed 30 May 13]; 20. Morgan, J. (2006), FSA closes GLG insider trading case, Risk.net [online], Available at: <http://www.risk.net/risk-magazine/news/1517719/fsa-closes-glg-insider-trading> [Accessed 3 June 13]

21. Financial Services Authority (2004) [online], Administrative Actions on Citibank, N.A. Japan Branch, Available at: <http://www.fsa.go.jp/news/e20040917-3.html>; [Accessed 3 June 13]

22. Citigroup (2004) [online], Citigroup CEO Prince Holds Press Conference in Japan, Available at: http://www.citigroup.jp/english/press_release/2004/20041025.pdf [Accessed 3 June 13]

23. Financial Services Authority (2005) [online], FSA Fines Citigroup £13.9 million (\$20.9mn) for Eurobond trades, Available at: <http://www.fsa.gov.uk/library/communication/pr/2005/072.shtml> [Accessed 3 June 13]

24. FinCEN (2004) [online], Amsouth Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/amsouthassessmentcivilmoney.pdf [Accessed 3 June 13]

25. FinCEN (2004) [online], Federal Reserve Board and Alabama Superintendent of Banks, Amsouth C&D and CMP: http://www.fincen.gov/news_room/ea/files/frb10122004.pdf [Accessed 3 June 13]

26. FinCEN (2004) [online], Riggs Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/riggssessment3.pdf [Accessed 3 June 13]

27. Federal Reserve Board (2004) [online], UBS AG Assessment of Civil Money Penalty, Available at: <http://www.federalreserve.gov/boarddocs/press/enforcement/2004/200405102/attachment.pdf> [Accessed 3 June 13]

28. SEC (2004) [online], UBS AG Form 6-K, Available at: <http://www.sec.gov/Archives/edgar/>

documents-show-secret-market-timing-arrangements [Accessed 3 June 13]

29. Baxter, Jr., T. (2004). Risk Management and Regulatory Failures at Riggs Bank and UBS: Lessons Learned (Testimony of Thomas C. Baxter, Jr.), Federal Reserve Bank of New York [online]. Available at: <http://www.newyorkfed.org/news/events/speeches/2004/bax040602.html> [Accessed 3 June 13]

30. OCC (2005) [online], City National Bank, Consent Order of Civil Money Penalty, Available at: <http://www.occ.gov/static/enforcement-actions/ea2005-17.pdf> [Accessed 5 June 13]

31. FinCEN (2005) [online], Oppenheimer & Company, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/oppeneimerassessment.pdf [Accessed 5 June 13]

32. FinCEN (2005) [online], Banco de Chile, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/bancodechile.pdf [Accessed 3 June 13]

33. OCC (2005) [online], Banco de Chile, C&D and Consent Order of Civil Money Penalty, Available at: <http://www.occ.gov/news-issuances/news-releases/2005/nr-occ-2005-11.html> [Accessed 3 June 13]

34. Federal Reserve Board (2005) [online], Banco de Chile, Cease and Desist Order, Available at: <http://www.federalreserve.gov/boarddocs/press/enforcement/2005/20050202/default.htm> [Accessed 3 June 13]

35. FinCEN (2011) [online], Pacific National Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/PacificNationalBankASSESSMENT.pdf [Accessed 5 June 13]

36. OCC (2011) [online], Pacific National Bank, Consent Order for Civil Money Penalty, Available at: <http://www.occ.gov/news-issuances/news-releases/2011/nr-ia-2011-32a.pdf> [Accessed 5 June 13]

37. OCC (2005) [online], Pacific National Bank, Consent Order Cease & Desist, Available at: <http://www.occ.gov/static/enforcement-actions/ea2005-165.pdf> [Accessed 5 June 13]

38. SEC (2005) [online], NYSE Administrative Proceeding (Settlement re: Censure and C&D), Available at: <http://www.sec.gov/litigation/admin/34-51524.pdf> [Accessed 3 June 13]

39. FinCEN (2005) [online], Arab Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/arab081705.pdf [Accessed 5 June 13]

40. OCC (2005) [online], Arab Bank, Consent Order for Civil Money Penalty, available at: <http://www.occ.gov/news-issuances/news-releases/2005/nr-ia-2005-80a.pdf> [Accessed 5 June 13]

41. Motley Rice [online], Arab Bank, 9-11 Civil Complaint (2004), Available at: <http://www.motleyrice.com/files/9-11-to-bankrupt-documents/almog-et-al-v-arab-bank-complaint-12-21-04.pdf> [Accessed 5 June 13]

42. Find Law [online], Arab Bank, Judge Gershon's Opinion and Order (2007), Available at: <http://news.findlaw.com/hdocs/docs/terrorism/almogab12907opn.html> [Accessed 5 June 13]

43. Am Law Daily [online], Arab Bank, Petition for Writ of Mandamus (2010), Available at: <http://amlawdaily.typepad.com/arabbankmandamus.pdf>

44. Wikipedia, Arab Bank, [online] [2013], Available at: http://en.wikipedia.org/wiki/Arab_Bank [Accessed 5 June 13]

45. FinCEN (2007) [online], Federal Register, Imposition of Special Measure Against Banco Delta Asia, Available at: http://www.fincen.gov/statutes_regs/patriot/pdf/bda_final_rule.pdf [Accessed 5 June 13]

46. Federal Reserve (2000) [online], Bank of New York, Written Agreement, Available at: <http://www.federalreserve.gov/boarddocs/press/enforcement/2000/20000208/attachment.pdf> [Accessed 5 June 13]

47. US Department of Justice (2005) [online], The Bank of New York Resolves Parallel Criminal Investigations Through Non-Prosecution Agreement With The US, Available at: <http://www.justice.gov/usao/nye/pr/2005/2005nov08.html> [Accessed 5 June 13]

48. Virginia Law Library [online], Bank of New York NPA (2003), Available at: http://lib.law.virginia.edu/Garrett/prosecution_agreements/pdf/bankofnewyork.pdf [Accessed 5 June 13]

49. Federal Reserve (2006) [online], Bank of New York, Written Agreement, Available at: <http://www.federalreserve.gov/newsevents/press/enforcement/enf20060424a1.pdf> [Accessed 5 June 13]

50. De La Merced, M. (2009). Bank of New York to Settle \$22.5 Billion Russian Lawsuit, Deal Book [online]. Available at: <http://dealbook.nytimes.com/2009/09/16/bank-of-new-york-settles-225-billion-russian-lawsuit/> [Accessed 5 June 13]

51. FinCEN (2006) [online], Beach Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/beachbank.pdf [Accessed 5 June 13]

52. FinCEN (2006) [online], Foster Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/foster.pdf [Accessed 5 June 13]

53. FinCEN (2006) [online], Israel Discount Bank of New York, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/fincen_assessment_of_civil_money_penalty.pdf [Accessed 5 June 13]

54. FinCEN (2006) [online], Liberty Bank of New York, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/liberty_assessment.pdf [Accessed 5 June 13]
55. FDIC (2006) [online], Liberty Bank of New York, Press Release, Available at: <http://www.fdic.gov/news/news/press/2006/pr06049.html> [Accessed 5 June 13]
56. FDIC (2006) [online], Liberty Bank of New York, CMP Consent Agreement, Available at: <https://www5.fdic.gov/EDOBlob/Mediator.aspx?UniqueID=48e0b9d2-c9ba-4e93-92bb-7890a38cb2c9> [Accessed 6 June 13]
57. NYS Banking Department (2006) [online], Liberty Bank of New York, Order of Assessment of CMP, Available at: <http://www.dfs.ny.gov/about/ea/ea060518.pdf> [Accessed 6 June 13]
58. FinCEN (2006) [online], BankAtlantic, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/bankatlantic_assessment.pdf [Accessed 6 June 13]
59. Office of Thrift Supervision (2006) [online], BankAtlantic, Consent Order to Cease and Desist, Available at: http://www.ots.treas.gov/_files/480236.pdf [Accessed 6 June 13]
60. Department of Justice (2006) [online], BankAtlantic Enters Into Deferred Prosecution Agreement, Forfeits \$10 Million To Resolve Money Laundering And Bank Secrecy Act Violations, Available at: http://www.justice.gov/opa/pr/2006/April/06_crm_248.html [Accessed 6 June 13]
61. FinCEN (2007) [online], Union Bank of California, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/ASSESSMENT_In_the_Matter_of_Union_Bank_of_California.pdf [Accessed 6 June 13]
62. OCC (2007) [online], Union Bank of California, Consent Order to a Civil Money Penalty and to Cease and Desist, Available at: <http://www.occ.gov/news-issuances/news-releases/2007/nr-ia-2007-95a.pdf> [Accessed 6 June 13]
63. Department of Justice (2007) [online], Union Bank of California Enters Into Deferred Prosecution Agreement and Forfeits \$21.6 Million to Resolve Bank Secrecy Act Violations, Available at: http://www.justice.gov/opa/pr/2007/September/07_crm_726.html [Accessed 6 June 13]
64. FinCEN (2007) [online], American Express Bank International, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/fincen_amex.pdf [Accessed 6 June 13]
65. Federal Reserve Board (2007) [online], American Express Bank International, C&D and CMP, Available at: <http://www.federalreserve.gov/newsevents/press/enforcement/enf20070806a1.pdf> [Accessed 6 June 13]
66. Department of Justice (2007) [online], American Express Bank International Enters Into Deferred Prosecution Agreement And Forfeits \$55 Million To Resolve Bank Secrecy Act Violations, Available at: http://www.justice.gov/opa/pr/2007/August/07_crm_584.html [Accessed 6 June 13]
- DPA: <http://www.justice.gov/criminal/pr/2007/08-06-07amex-charge-agreemnt.pdf> [Accessed 6 June 13]
67. NASD (2007) [online], NASD Fines Bank of America Investment Services, Inc. \$3 Million for Failing to Comply With Anti-Money Laundering Rules in Connection With High Risk Accounts, Available at: <http://www.finra.org/Newsroom/NewsReleases/2007/P018404> [Accessed 6 June 13]
68. Johnston, D. (2006). Bank of America Acknowledges Illicit Funds Moved Through a Manhattan Branch [online]. Available at: http://www.nytimes.com/2006/09/28/business/28bank.html?_r=0 [Accessed 6 June 13]
69. OCC (2007) [online], The International Bank of Miami, Order for a Civil Money Penalty, Available at: <http://www.occ.gov/static/enforcement-actions/ea2007-011.pdf> [Accessed 6 June 13]
70. Bank of Israel (2008) [online], Decision of the Banking Corporations Sanctions Committee regarding infringement of the provisions under the Prohibition on Money Laundering Law by Israel Discount Bank Ltd., Available at: <http://www.boi.org.il/en/NewsAndPublications/PressReleases/Pages/081103e.aspx> [Accessed 6 June 13]
71. FDIC (2008) [online], Mizrahi Tefahot Bank, Ltd., Order to Cease and Desist, Available at: <http://www.fdic.gov/bank/individual/enforcement/2008-08-02.pdf> [Accessed 6 June 13]
72. FDIC (2008) [online], Mizrahi Tefahot Bank, Ltd., Order to Pay Civil Money Penalty, Available at: <http://www.fdic.gov/bank/individual/enforcement/2011-01-30.pdf> [Accessed 6 June 13]
73. SEC (2008) [online], E*Trade Administrative Proceeding (Cease and Desist), Available at: <http://sec.gov/litigation/admin/2008/34-58250.pdf> [Accessed 6 June 13]
74. OCC (2007) [online], United Bank for Africa, Consent Order to Cease and Desist, Available at: <http://www.occ.gov/static/enforcement-actions/ea2007-003.pdf> [Accessed 6 June 13]
75. OCC (2007) [online], United Bank for Africa, Consent Order for a Civil Money Penalty, Available at: <http://www.occ.gov/static/enforcement-actions/ea2007-039.pdf> [Accessed 6 June 13]
76. OCC (2008) [online], Bank for Africa, Consent Order to Cease and Desist, Available at: <http://www.occ.gov/static/enforcement-actions/ea2008-007.pdf> [Accessed 6 June 13]
77. OCC (2008) [online], United Bank for Africa, Consent Order for a Civil Money Penalty, Available at: <http://www.occ.gov/static/enforcement-actions/ea2008-029.pdf> [Accessed 6 June 13]
78. FinCEN (2008) [online], United Bank for Africa, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/UBAAssessment.pdf [Accessed 6 June 13]
79. FinCEN (2008) [online], Sigue Corporation, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/sigue_assement_final.pdf [Accessed 6 June 13]
80. Virginia Law Library [online], Sigue Corporation DPA (2008), Available at: <http://www.law.virginia.edu/pdf/faculty/garrett/sigue.pdf> [Accessed 6 June 13]
81. O'Neill, M. (2012). Japanese bank fined over suspicious dealings, South China Morning Post [online]. Available at: <http://www.scmp.com/article/543648/japanese-bank-fined-over-suspicious-dealings> [Accessed 6 June 13]
82. Financial Services Authority (2010) [online], Winterflood Securities Limited, Final Notice, Available at: <http://www.fsa.gov.uk/pubs/2010/winterflood.pdf> [Accessed 6 June 13]
83. Financial Services Authority (2010) [online], Winterflood Securities Limited, Statement of Case, Available at: <http://www.fsa.gov.uk/pubs/2010/winterflood.pdf> and Background to share ramping scheme, Available at: http://www.fsa.gov.uk/pubs/2010/winterflood_fei.pdf [Accessed 6 June 13]
84. AFP-Google (2008) [online], French regulator fines Société Générale for rogue trade, Available at: <http://afp.google.com/article/ALEqM5gVId1yJjFveoMCdJVDzClzwqrQuW> [Accessed 6 June 13]
85. Financial Services Authority (2009) [online], FSA fines Aon Limited £5.25m for failings in its anti-bribery and corruption systems and controls, Available at: <http://www.fsa.gov.uk/library/communication/pr/2009/004.shtml> [Accessed 6 June 13]
86. Financial Services Authority (2009) [online], Aon Limited, Final Notice, Available at: <http://www.fsa.gov.uk/pubs/2010/aon.pdf> [Accessed 6 June 13]
87. FinCEN (2009) [online], Doha Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/Doha.pdf [Accessed 6 June 13]
88. OCC (2009) [online], Doha Bank, Consent Order for Civil Money Penalty, Available at: <http://www.occ.gov/static/enforcement-actions/ea2009-056.pdf> [Accessed 6 June 13]
89. OCC (2006) [online], Doha Bank, Consent Order to Cease and Desist, Available at: <http://www.occ.gov/static/enforcement-actions/ea2006-107.pdf> [Accessed 6 June 13]
90. FINRA (2009) [online], E*Trade Units Fined \$1 Million for Inadequate Anti-Money Laundering Programme, Available at: <http://www.finra.org/Newsroom/NewsReleases/2009/P117667> [Accessed 6 June 13]
91. Department of Justice (2009) [online], Credit Suisse Agrees to Forfeit \$536 Million in Connection with Violations of the International Emergency Economic Powers Act and New York State Law, Available at: <http://www.justice.gov/opa/pr/2009/December/09-ag-1358.html> [Accessed 6 June 13]
- Factual Statement: <http://www.justice.gov/criminal/pr/documents/12-16-09-CreditSuisse-factualstatement.pdf> [Accessed 6 June 13]
92. Department of Justice (2009) [online], Credit Suisse, Deferred Prosecution Agreement:, Available at: <http://www.justice.gov/criminal/pr/documents/12-16-09-deferred-%20prosecution-%20agreement.pdf> [Accessed 6 June 13]
93. Department of Justice (2009) [online], Lloyds TSB Bank Plc Agrees to Forfeit \$350 Million in Connection with Violations of the International Emergency Economic Powers Act, Available at: <http://www.justice.gov/opa/pr/2009/January/09-crm-023.html> [Accessed 7 June 13]
94. Department of the Treasury (2009) [online], Lloyds TSB Bank, plc Settlement Agreement, Available at: http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/lloyds_agreement.pdf [Accessed 7 June 13]
95. Gibson Dunn [online], Lloyds TSB Bank, plc, DPA with Department of Justice (2009), Available at: <http://www.gibsondunn.com/publications/Documents/LloydsTSB-DeferredProsecutionAgmt010909.pdf> [Accessed 7 June 13]
- The Factual Statement accompanying DPA: <http://www.gibsondunn.com/publications/Documents/LloydsTSB-DPAgmt-FactualStatment.pdf> [Accessed 7 June 13]
96. SEC (2009) [online], SEC Charges R. Allen Stanford, Stanford International Bank for Multi-Billion Dollar Investment Scheme, Available at: <http://www.sec.gov/news/press/2009/2009-26.htm> [Accessed 7 June 13]
97. Department of Justice (2009) [online], Stanford Indictment, Available at: <http://www.justice.gov/criminal/vns/docs/2009/jun/06-18-09Stanford.pdf> [Accessed 7 June 13]
98. FBI (2012) [online], Allen Stanford Gets 110 years for Orchestrating \$7 Billion Investment Fraud Scheme, Available at: <http://www.fbi.gov/houston/press-releases/2012/allen-stanford-gets-110-years-for-orchestrating-7-billion-investment-fraud-scheme> [Accessed 7 June 13]

99. Department of Justice (2009) [online], Justice Department & IRS Announce Results of UBS Settlement & Unprecedented Response in Voluntary Tax Disclosure Programme, Available at: <http://www.justice.gov/opa/pr/2009/November/09-tax-1241.htm> [Accessed 7 June 13]
100. Department of Justice (2009) [online], UBS Enters Into Deferred Prosecution Agreement, Available at: <http://www.justice.gov/tax/txdv09136.htm> [Accessed 7 June 13]
- Information: http://www.justice.gov/tax/UBS_Filed_Stamped_Information.pdf [Accessed 7 June 13]
- DPA: http://www.justice.gov/tax/UBS_Signed_Deferred_Prosecution_Agreement.pdf [Accessed 7 June 13]
101. Department of Justice (2008) [online], UBS AG, John Doe Summons, Available at: http://www.justice.gov/tax/UBS_Order.pdf [Accessed 7 June 13]
102. Department of the Treasury (2009) [online], Australia and New Zealand Banking Group Ltd. Settlement Agreement, Available at: http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/anz_08242009.pdf [Accessed 7 June 13]
103. CFTC (2009) [online], Amaranth Entities Ordered to Pay a \$7.5 Million Civil Fine in CFTC Action Alleging Attempted Manipulation of Natural Gas Futures Prices, Available at: <http://www.cftc.gov/PressRoom/PressReleases/pr5692-09> [Accessed at 7 June 13]
104. Rucker, P. (2013). US court rules FERC cannot fine Amaranth trader, Thomson Reuters [online]. Available at: http://newsandinsight.thomsonreuters.com/Legal/News/2013/03_-_March/U_S__court_rules_FERC_can-not_fine_Amaranth_trader/ [Accessed 7 June 13]
105. Department of Justice (2010) [online], Former ABN Bank N.V. Agrees to Forfeit \$500 Million in Connection with Conspiracy to Defraud the US and with Violation of the Bank Secrecy Act, Available at: <http://www.justice.gov/opa/pr/2010/May/10-crm-548.html> [Accessed 7 June 13]
106. FBI (2010) [online], Former ABN AMRO Bank N.V. Agrees to Forfeit \$500 Million in Connection with Conspiracy to Defraud the US and with Violation of the Bank Secrecy Act, Available at: <http://www.fbi.gov/washington/dc/press-releases/2010/wfo051010.htm> [Accessed 7 June 13]
107. FinCEN (2005) [online], ABN Amro, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/abn_assessment.pdf [Accessed 3 June 13]
108. Virginia Law Library [online], ABN Amro DPA (2010), Available at: DPA: http://lib.law.virginia.edu/Garrett/prosecution_agreements/pdf/ABN_AMRO.pdf [Accessed 7 June 13]
109. OCC (2010) [online], Wachovia Bank, Consent Order to Cease and Desist, Available at: <http://www.occ.gov/news-issuances/news-releases/2010/nr-occ-2010-30b.pdf> [Accessed 10 June 13]
110. OCC (2010) [online], Wachovia Bank, Consent Order for a Civil Money Penalty, Available at: <http://www.occ.gov/news-issuances/news-releases/2010/nr-occ-2010-30c.pdf> [Accessed 10 June 13]
111. FinCEN (2010) [online], Wachovia Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/100316095447.pdf [Accessed 10 June 13]
112. Department of Justice (2010) [online], Wachovia Bank, Deferred Prosecution Agreement, Available at: <http://www.justice.gov/usaof/fts/PressReleases/Attachments/100317-02.Agreement.pdf> [Accessed 10 June 13]
- DOJ Factual Statement, Available at: <http://www.justice.gov/usaof/fts/PressReleases/Attachments/100317-02.Statement.pdf> [Accessed 10 June 13]
113. New York County District Attorney's Office (2010) [Online], District Attorney Vance Announces \$298 Million Settlement with Barclays, Available at: <http://manhattanda.org/press-release/district-attorney-vance-announces-298-million-settlement-barclays> [Accessed 11 June 13]
114. Wall Street Journal (2010) [online], Barclays Bank PLC, Deferred Prosecution Agreement, Available at: <http://online.wsj.com/public/resources/documents/081710barclaysruling.pdf> [Accessed 11 June 13]
115. Department of the Treasury (2010) [online], Barclays Bank PLC Settlement Agreement, Available at: <http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/08182010.pdf> [Accessed 11 June 13]
116. Deutsche Bank (2010) [online] US Department of Justice Settlement Agreement. Available at: <<http://www.justice.gov/tax/usaopress/2010/deutschebankpr.pdf>> [Accessed 8 September 2013]
117. FinCEN (2010) [online], Pamrapo Savings Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/PamrapoAssessment.pdf [Accessed 7 June 13]
118. Office of Thrift Supervision (2010) [online], Pamrapo Savings Bank, Order of Assessment of a Civil Money Penalty, Available at: <http://files.ots.treas.gov/482129.pdf> [Accessed 10 June 13]
119. Department of Justice (2010) [online], Pamrapo Savings Bank of New Jersey Pleads Guilty to Conspiracy to Commit Bank Secrecy Act Violations and Forfeits \$5 Million, Available at: <http://www.justice.gov/opa/pr/2010/March/10-crm-335.html> [Accessed 10 June 13]
120. Financial Services Authority (2010) [online], Goldman Sachs International, Final Notice, Available at: http://www.fsa.gov.uk/pubs/final/goldman_sachs_int.pdf [Accessed 10 June 13]
121. New York Law Journal (2011) [online], Goldman Sachs Group, Inc., Motion to Dismiss: <http://www.nylj.com/nylawyer/adgifs/decisions/062512defense.pdf> [Accessed 10 June 13]
122. SEC (2010) [online], Goldman Sachs & Co., Complaint, Available at: <http://www.sec.gov/litigation/complaints/2010/comp21489.pdf> [Accessed 10 June 13]
123. SEC (2010) [online], Goldman Sachs & Co., Consent, Available at: <http://www.sec.gov/litigation/litreleases/2010/consent-pr2010-123.pdf> [Accessed 10 June 13]
124. FINRA (2010) [online], FINRA Sanctions Trillium Brokerage Services, LLC, Director of Trading, Chief Compliance Officer, and Nine Traders \$2.26 Million for Illicit Equities Trading Strategy, Available at: Source: <http://www.finra.org/Newsroom/NewsReleases/2010/P121951> [Accessed 10 June 13]
125. FINRA (2010) [online], Trillium Brokerage Services, LLC, Letter of Acceptance, Waiver and Consent, Available at: <http://www.finra.org/web/groups/industry/@ip/@enf/@ad/documents/industry/p122044.pdf> [Accessed 10 June 13]
126. Wray, R. (2010). RBA handed FSA's biggest fine for lapses over money laundering rules, The Guardian [online]. Available at: <http://www.guardian.co.uk/business/2010/aug/03/royal-bank-of-scotland-fsa-biggest-fine> [Accessed 10 June 13]
127. SEC (2011) [online], SEC Charges Merrill Lynch for Misusing Customer Order Information and Charging Undisclosed Trading Fees, Available at: <http://www.sec.gov/news/press/2011/2011-22.htm> [Accessed 11 June 13]
128. SEC (2011) [online], Merrill Lynch, Pierce, Fenner & Smith Incorporated, Administrative and Cease-and-Desist Proceedings, Available at: <http://www.sec.gov/litigation/admin/2011/34-63760.pdf> [Accessed 12 June 13]
129. FinCEN (2011) [online], FDIC, FinCEN and the State of Florida Office of Financial Regulation Assess Civil Money Penalties Against Ocean Bank, Available at: http://www.fincen.gov/news_room/nr/html/20110822.html [Accessed 12 June 13]
130. FDIC (2011) [online], Ocean Bank, Order to Pay, Available at: <http://www.fdic.gov/news/news/press/2011/pr11140a.pdf> [Accessed 12 June 13]
131. FinCEN (2011) [online], Ocean Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/08222011_OceanBank_ASSESSMENT.pdf [Accessed 12 June 13]
132. Florida OFR (2011) [online], State Regulator Confident Ocean Bank will Comply with Regulatory Agreement, Available at: <http://www.florfr.com/PressReleaseDetail.aspx?id=3931> [Accessed 12 June 13]
133. Department of Justice (2011) [online], Ocean Bank, Deferred Prosecution Agreement, Available at: <http://www.justice.gov/usao/fts/PressReleases/Attachments/110822-01.DPA.pdf> [Accessed 12 June 13]
134. OCC (2011) [online], OCC and FinCEN Assess Civil Money Penalties Against Pacific National Bank, Miami, Florida, Available at: <http://www.occ.gov/news-issuances/news-releases/2011/nr-ia-2011-32.html> [Accessed 12 June 13]
135. OCC (2011) [online], Pacific National Bank, Consent Order for a Civil Money Penalty, Available at: <http://www.occ.gov/news-issuances/news-releases/2011/nr-ia-2011-32a.pdf> [Accessed 12 June 13]
136. FinCEN (2011) [online], Pacific National Bank, Assessment of Civil Money Penalty, Available at: <http://www.occ.gov/news-issuances/news-releases/2011/nr-ia-2011-32b.pdf> [Accessed 12 June 13]
137. FinCEN (2011) [online], Zions First National Bank, Assessment of Civil Money Penalty, Available at: Source: http://www.fincen.gov/news_room/ea/files/ZionsAssessment.pdf [Accessed 12 June 13]
138. OCC (2011) [online], Zions First National Bank, Consent Order, Available at: Source: <http://occ.gov/news-issuances/news-releases/2011/nr-occ-2011-16a.pdf> [Accessed 12 June 13]
139. FDIC (2011) [online], Mizrahi Tefahot Bank, Ltd., Order to Pay Civil Money Penalty, Available at: <http://www.fdic.gov/bank/individual/enforcement/2011-01-30.pdf> [Accessed 17 June 13]
140. FDIC (2008) [online], Mizrahi Tefahot Bank, Ltd., Order to Cease and Desist, Available at: C&D: <http://www.fdic.gov/bank/individual/enforcement/2008-08-02.pdf> [Accessed 17 June 13]
141. Department of the Treasury (2011) [online], JPMorgan Chase Bank N.A. Settles Apparent Violations of Multiple Sanctions Programmes, Available at: <http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20110825.aspx> [Accessed 17 June 13]
142. Department of the Treasury (2011) [online], JPMorgan Chase Bank N.A., Settlement Agreement, Available at: <http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/jpmorgan.pdf> [Accessed 17 June 13]
143. BBC News (2011) [online], Deutsche Bank charged in South Korea over stock rout, Available at: <http://www.bbc.co.uk/news/business-14611852> [Accessed 17 June 13]
144. Financial Services Commission (2011) [online], Deutsche Bank, Unfair Trading Investigation and Results, Available at: <http://www.fsc.go.kr/downManager?bbsid=BBS0048&no=73803> [Accessed 17 June 13]

145. Lebanese Commercial Bank (2011) [online] Available at: <<http://www.justice.gov/usao/nys/pressreleases/June13/LCBSettlementPR/U.S.%20v.%20lebanese%20canadian%20Bank%20Settlement%20Order.pdf>> [Accessed 8 September 2013]
146. Financial Services Authority (2012) [online], Turkish Bank (UK) Ltd fined £294,000 for money laundering failings, Available at: <http://www.fsa.gov.uk/library/communication/pr/2012/081.shtml> [Accessed 17 June 13]
147. Bank of Israel (2012) [online], Decision regarding infringements by Mizrahi-Tefahot Bank of directives under the Prohibition on Money Laundering Law, Available at: <http://www.bankisrael.gov.il/en/NewsAndPublications/PressReleases/Pages/20092012.aspx> [Accessed 17 June 13]
148. Financial Services Authority (2012) [online], Coutts fined £8.75mio for anti-money laundering control failings, Available at: <http://www.fsa.gov.uk/library/communication/pr/2012/032.shtml> [Accessed 17 June 13]
149. Financial Services Authority (2012) [online], FSA fines Habib Bank AG Zurich £525,000 and money laundering reporting officer £17,500 for anti-money laundering control failings, Available at: <http://www.fsa.gov.uk/library/communication/pr/2012/055.shtml> [Accessed 17 June 13]
150. Department of Justice (2012) [online], HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit \$1.256 Billion in Deferred Prosecution Agreement, Available at: <http://www.justice.gov/opa/pr/2012/December/12-crm-1478.html> [Accessed 17 June 13]
151. Gibson Dunn [online], HSBC Bank USA, N.A., Information and DPA with Department of Justice (2012), Available at: http://www.gibsondunn.com/publications/Documents/HSBC_DPA.pdf [Accessed 17 June 13]
152. OCC (2012) [online], OCC Assesses \$500 Million Civil Money Penalty Against HSBC Bank USA, N.A., Available at: <http://www.occ.gov/news-issuances/news-releases/2012/nr-occ-2012-173.html> [Accessed 17 June 13]
153. FinCEN (2012) [online], HSBC Bank USA N.A., Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/news_room/ea/files/HSBC_ASSESSMENT.pdf [Accessed 17 June 13]
154. Department of the Treasury (2012) [online], Treasury Department Reaches Landmark Settlement with HSBC, Available at: <http://www.treasury.gov/press-center/press-releases/Pages/tg1799.aspx> [Accessed 17 June 13] and HSBC Holdings plc., Settlement Agreement, Available at: http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/121211_HSBC_Settlement.pdf [Accessed 17 June 13]
155. BBC News (2012) [online], UBS fined £29.7m by FSA over Kweku Adoboli case, Available at: <http://www.bbc.co.uk/news/business-20492017> [Accessed 17 June 13]
156. Department of Justice (2012) [online], Swiss Bank Indicted on US Tax Charges, Available at: <http://www.justice.gov/opa/pr/2012/February/12-tax-153.html> [Accessed 17 June 13]
157. Gibson Dunn [online], ING Bank, N.V., DPA with Department of Justice (2012), Available at: Sources: DPA: http://www.gibsondunn.com/publications/Documents/INGBankNV_DPA.PDF [Accessed 17 June 13]
158. Department of the Treasury (2012) [online], Settlement Agreement between the US Department of the Treasury's Office of Foreign Assets Control and ING Bank, N.V., Available at: <http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20120612.aspx> [Accessed 17 June 13] and Settlement Agreement, Available at: http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/06122012_ingroup_agreement.pdf [Accessed 17 June 13]
159. NY State Department of Financial Services (2012) [online], Standard Chartered Bank, Order, Available at: <http://www.dfs.ny.gov/about/ea/ea120806.pdf> [Accessed 18 June 13]
160. NY State Department of Financial Services (2012) [online], Standard Chartered Bank, Consent Order, Available at: <http://www.dfs.ny.gov/about/ea/ea120921.pdf> [Accessed 18 June 13]
161. Department of the Treasury (2012) [online], Settlement Agreement between the US Department of the Treasury's Office of Foreign Assets Control and Standard Chartered Bank, Available at: <http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20121210.aspx> [Accessed 18 June 13] and Settlement Agreement, Available at: http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/121210_SCB_Settlement.pdf [Accessed 18 June 13]
162. Federal Reserve Board (2012) [online], Standard Chartered Bank, Press Release re: Cease and Desist Order and Order of Assessment of a Civil Money Penalty, Available at: <http://www.federalreserve.gov/newsreleases/press/enforcement/20121210a.htm> [Accessed 18 June 13] and Department of Justice (2012) [online], Standard Chartered Bank Agrees to Forfeit \$227 Million for Illegal Transactions with Iran, Sudan, Libya, and Burma, Available at: <http://www.justice.gov/opa/pr/2012/December/12-crm-1467.html> [Accessed 18 June 13]
163. New York County District Attorney's Office (2012) [Online], Standard Chartered Bank Reaches \$327 Million Settlement for Illegal Transactions, Available at: <http://manhattanda.org/press-release/standard-chartered-bank-reaches-327-million-settlement-illegal-transactions> [Accessed 18 June 13]
164. FinCEN (2012) [online], FDIC and FinCEN Assess Civil Money Penalty Against First Bank of Delaware,

- Available at: http://www.finncen.gov/news_room/nr/html/20121119.html [Accessed 18 June 13]
165. SEC (2012) [online], SEC Charges Germany-Based Allianz SE with FCPA Violations, Available at: <http://www.sec.gov/news/press/2012/2012-266.htm> [Accessed 18 June 13]
166. Wikipedia, Libor scandal, [online] [2013], Available at: http://en.wikipedia.org/wiki/Libor_scandal [Accessed 21 June 13]
167. Albergotti, R. and Eaglesham, J. (2012). 9 More Banks Subpoenaed Over Libor, Wall Street Journal [online]. Available at: <http://online.wsj.com/article/SB10001424052970203897404578079413742864842.html> [Accessed 21 June 13]
168. Alper, A. and Ridley, R. (2012). Barclays paying \$453 million to settle Libor probe, Reuters [online]. Available at: <http://www.reuters.com/article/2012/06/27/us-barclays-libor-idUSBRE85Q0J720120627> [Accessed 21 June 13]
169. UBS (2012) [online], Libor settlements, Available at: http://www.ubs.com/global/en/about_ubs/media/global/libor.html [Accessed 21 June 13]
170. RBS (2013) [online], RBS reaches Libor settlements, Available at: <http://www.investors.rbs.com/newsitem?item=1278540897095016> [Accessed 21 June 13]
171. CFTC (2013) [online], CFTC Charges ICAP Europe Limited, a Subsidiary of ICAP plc, with Manipulation and Attempted Manipulation of Yen Libor, Available at: <http://www.cftc.gov/PressRoom/PressReleases/pr6708-13> [Accessed 14 October 13]
172. Enrich, D. and Strasburg, J. (2013). Rabobank Is Fined, CEO Is Out in Libor Settlement, Wall Street Journal [online]. Available at: http://online.wsj.com/news/articles/SB10001424052702303471004579165293824297108?mod=djemTMB_h [Accessed 2 December 13] Department of Justice (2013) [online], Rabobank Admits Wrongdoing in Libor Investigation, Agrees to Pay \$325 Million Criminal Penalty, Available at: <http://www.justice.gov/opa/pr/2013/October/13-crm-1147.html> [Accessed 2 December 13]
173. EU Commission (2013) Press Release. Available at: <http://europa.eu/rapid/press-release_IP-13-1208_en.htm> [Accessed 15th December 2013].
174. Department of the Treasury (2012) [online], National Bank of Abu Dhabi Settles Potential Liability for Apparent Violations of the Sudanese Sanctions Regulations, Available at: http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/06142012_nbad.pdf [Accessed 18 June 13]
175. US Department of Justice (2012) [online]: Moneygram International Inc. Admits Anti-Money Laundering and Wire Fraud Violations, Forfeits \$100 Million in Deferred Prosecution: Available at <<http://www.justice.gov/opa/pr/2012/November/12-crm-1336.html>> [Accessed on 31st December 2013]
176. SEC (2013) [online], CR Instrinsic Agrees to Pay More than \$600 Million in Largest-Ever Settlement for Insider Trading Case, Available at: <http://www.sec.gov/news/press/2013/2013-41.htm> [Accessed 21 June 13]
177. FSA Final Notice (2013) [online] Available at: <<http://www.fca.org.uk/static/documents/final-notices/efg-privalebank.pdf>> [Accessed 8 September 2013]
178. UBS France: Swissinfo.ch 2013 [online] Available at: <<http://www.swissinfo.ch/eng/detail/content.html?cid=36272254>> [Accessed 8 September 2013] and ACP Notice in French Available at: <http://www.acp-banque-france.fr/fi/leadmin/user_upload/acpCommunication/Communiques%20de%20pressc/20130626-cp-decision-de-la-commission-des-sanctions.pdf> [Accessed 8 September 2013]
179. HSBC Argentina: Insightcrime 2013 [online] Available at: <<http://www.m.insightcrime.org/pages/article/4288>> [Accessed 8 September 2013]
180. HSBC Mexico: CNS Business: 2013 [online] Available at: <<http://www.cnsbusiness.com/content/cima/finally-pullshsbc-mexico-license>> [Accessed 8 September 2013]
- 181 & 182. Department of the Treasury (2012) [online], Bank of Tokyo-Mitsubishi UFJ, Ltd. Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programmes, [online] Available at: <http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20121212_btmu.pdf> [Accessed 18 June 13] and 2013 [online] Available at: <http://dealbook.nytimes.com/2013/06/20/japans-largest-bank-to-pay-250-million-fine-for-iran-deals/?_r=0> [Accessed 8 September 2013]
183. Barclays - Wingfield, B. (2012). Barclays' Energy Trading in Record \$470 Million US Fine, Bloomberg [online]. Available at: <http://www.bloomberg.com/news/2012-11-01/u-s-proposes-record-penalty-for-barclays-energy-trades.html> [Accessed 21 June 13]
184. Nordea (2013) [online] Swedish FSA Press Release: Available at: <http://www.frankics.org/cms/pdfs/sweden/SFSASFSANorden_PressRelease_16.4.13.pdf> [Accessed 8 September 2013]
185. Panther Energy Trading (2013) [online] Available at: <<http://www.cftc.gov/PressRoom/PressReleases/pr6649-13>> [Accessed 8 September 2013]

186. Oppenheimer & Co 2013 [online] <<http://www.finra.org/Newsroom/NewsReleases/2013/P314981>> and <<http://www.finra.org/web/groups/industry/@ip/@enf/@ad/documents/industry/p315930.pdf>> [Accessed 8 September 2013]
187. AMEX: OFAC Enforcement Notice: 2013 [online] Available at: <http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20130722_american_express-trs.pdf> [Accessed 8 September 2013]
188. Guaranty Trust Bank 2013 [online] Available at: <<http://uk.reuters.com/article/2013/08/09/uk-gtbank-fi-ne-idUKBRE978ORJ20130809>> [Accessed 8 September 2013]
189. JP Morgan/JP Morgan Ventures Energy Corporation 2013 [online] Available at: <<http://www.ferc.gov/media/newsreleases/20013/2013-07-30-13.asp#UiwpLqN5MKO>> [Accessed 8 September 2013]
190. Sidel, R., Patterson, S. and Eaglesham, J. (2013). JP Morgan Faces a Hard-Line SEC, Wall Street Journal [online]. Available at: <http://online.wsj.com/news/articles/SB10001424127887324807704579084912809151456> [Accessed 14 October 13]
191. FinCEN (2013) [online], FinCEN Penalizes New Jersey Community Bank for Risky Dealings with Foreign Money Exchanges, Available at: http://www.fincen.gov/news_room/nr/html/20130924.html [Accessed 2 December 13]
192. OCC (2013) [online], OCC Assesses \$10 Million Civil Money Penalty Against TCF National Bank, Bank Secrecy Act Violations Cited, Available at: <http://www.occ.treas.gov/news-issuances/news-releases/2013/nr-occ-2013-18.html> [Accessed 2 December 13]
193. FinCEN (2013) [online], TD Bank, Assessment of Civil Money Penalty, Available at: http://www.fincen.gov/pdf/TD_ASSESSMENT_09222013.pdf [Accessed 2 December 13] SEC (2013) [online], SEC Charges TD Bank and Former Executive for Roles in Rothstein Ponzi Scheme in South Florida (Press Release with links to Order and Complaint), Available at: <http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539827946> [Accessed 2 December 13]
194. Reserve Bank of India (2013) [online], RBI penalises six banks, Available at: http://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=29372 [Accessed 2 December 13]
195. Worldradio.ch (2013) [online], 3 banks fined in Ben-Ali regime scandal, Available at: <http://www.worldradio.ch/news/local-news/3-banks-fined-in-ben-ali-regime-scandal/> [Accessed 2 December 13]
196. US Treasury (2013) Available at: <<http://www.treasury.gov/press-center/press-releases/Pages/jl2239.aspx>>
197. FCA Final Order: Available at <<http://www.fca.org.uk/news/firm-fined-18million-for-unacceptable-approach-to-bribery-corruption-risks-from-overseas-payments>> [Accessed 20 March 2014]
198. Enrich, D. (2013). Libor Case Ensnares More Banks, Wall Street Journal [online]. Available at: <http://online.wsj.com/article/SB10001424127887323893504578556941091595054.html> [Accessed 21 June 13]
199. Enrich, D. (2013). Regulators Look for Three More Libor Settlements, Wall Street Journal [online video]. Available at: <http://live.wsj.com/video/regulators-look-for-three-more-libor-settlements/7C71D601-3B74-4A27-B6CD-BBC6199A1391.html#.7C71D601-3B74-4A27-B6CD-BBC6199A1391> [Accessed 21 June 13]
200. Broom, G. and Logutenkova, E. (2013). Credit Suisse, Baer Seen Facing Delay in US Tax Deal, Bloomberg [online]. Available at: <http://www.bloomberg.com/news/2013-06-19/credit-suisse-baer-seen-facing-delay-in-u-s-taxdeal-on-vote.html> [Accessed 21 June 13]
201. Scannell, K. and Simonian, H. (2013). US probe into tax evasion widens, Financial Time [online]. Available at: <http://www.ft.com/intl/cms/s/0/88bc1474-42a9-11e0-8b34-00144feabdc0.html#axzz2WrQmNXhC> [Accessed 21 June 13]
202. Mustoe, H. (2013). Barclays Saudi Probe Adds to CEO Jenkins's Regulatory Woe, Bloomberg [online]. Available at: <http://www.bloomberg.com/news/2012-11-12/barclays-saudi-investigation-adds-to-jenkins-s-regulatory-woes.html> [Accessed 21 June 13]
203. Schafer, D., Bingham, C. and Kerr, S. (2013). Barclays in Qatar Loan Probe, Financial Times [online]. Available at: <http://www.cnbc.com/id/100425860> [Accessed 21 June 13]
204. Silver-Greenberg, J., Protess, B., and Barboza, D. (2013). Hiring in China by JP Morgan Under Scrutiny, New York Times [online]. Available at: http://dealbook.nytimes.com/2013/08/17/hiring-in-china-by-jpmorgan-under-scrutiny/?_r=0 [Accessed 2 December 13]
205. SEC (2013) [online], SEC Charges Traders in Massive Kickback Scheme Involving Venezuelan Official, Available at: <http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171514248> [Accessed 2 December 13]
2. Bank of England Waking Shark II; Desktop Cyber Exercise; Report to participants; Tuesday 12 November 2013. Available at <http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=3&sqi=2&ved=0CD0QFjAC&url=http%3A%2F%2Fwww.bankofengland.co.uk%2Ffinancialstability%2Ffsc%2Fdocuments%2Fwakinshark2report.pdf&ei=bQwrU_7EEaboywPV1YIg&usg=AFQjCNHhgJO2oVh-D1Xi2tBJi3RzjD3Yvg> [Accessed 20 March 14]
3. The Basel Committee on Banking Supervision: Sound management of risks related to money laundering and financing of terrorism. Available at: <<http://www.bis.org/publ/bcbs275.htm>> [Accessed 20 March 14]
4. OCC and FinCEN Orders: Available at <<http://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-1.html>> [Accessed 20 March 2014]
5. FCA Order: Available at <<http://www.fca.org.uk/news/standard-bank-plc-fined-for-failures-in-its-antimoney-laundering-controls>> [Accessed 20 March 2014]
6. FCA Final Notice: Available at <<http://www.fca.org.uk/your-fca/documents/final-notices/2014/7722656-canadian-inc>> [Accessed 20 March 2014]
7. SEC Press Release: available at <<http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370540816517#.UyqBZqN5mK0>> [Accessed 20 March 2014]
8. Senate Hearings Report: Available at <<http://www.hsgac.senate.gov/download/?id=DD609B36-94AB-44B5-AABA-97B2AB08E058>> [Accessed 20 March 2014]
9. FINRA Fines Brown Brothers Harriman; Available at: <<https://www.finra.org/Newsroom/NewsReleases/2014/P443442>> (20 March 2014)
10. FT Article: Available at <<http://www.ft.com/cms/s/2/7a9b85b4-4af8-11e3-8c4c-00144feabdc0.html#axzz2sG2XPJec>> [Accessed 20 March 2014]

Breaking News

1. EU Anti-Corruption report including country chapters, Eurobarometer surveys, factsheets and questions and answers: Available at <<http://ec.europa.eu/anti-corruption-report>> [Accessed 20 March 2014]

Abbreviations

Acronym	Means
ABC, ABC Programme, anti-bribery, anti-corruption	Anti-bribery and Corruption, Anti-Corruption
AML, AML Programme	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and Counter Financing of Terrorism
Anti-Fraud Programme, anti-fraud	Anti-Fraud programme
CDD	Customer Due Diligence
EU	European Union
FIU	Financial Intelligence Units
FTO	Foreign Terrorist Organisations
KYC	Know Your Customer
ML, ML/FT (not TF)	Money laundering, Money laundering and Financing of Terrorism
MSB	Money Service Business
NPO	Not for Profit Organisations
PEP	Politically Exposed Persons
RBA	Risk Based Approach
SAR	Suspicious Activity Reporting
SST	State Sponsor of Terrorism
SWF	Sovereign Wealth Funds
UN	United Nations
UNSCR	United Nations Security Council Resolution
WMD	Weapons of Mass Destruction
WWI or WWII	World War

Index

Introduction

- Five Recommendations to Effectively combat Money Laundering, 5-10
- Facts & Figures, 11-12
- What is Money Laundering, 13-18

Part 1

Section 1 - Money Laundering Crimes

- Introduction, 21-22
- Bribery & Corruption, 23-28
 - Petty Corruption, 26
 - Private Corruption, 26
 - Organised Corruption, 27
 - Grand Corruption, 27
 - Counterfeiting & Piracy of Products, 29-34
 - Counterfeit Drugs, 31
 - Counterfeit Electronics, 31
 - Software Piracy, 32
 - Counterfeit Foods, 32
 - Counterfeit Auto Parts, 33
 - Counterfeit Toys, 33
 - Movie and Music Piracy, 33
 - Counterfeit Shoes, 34
 - Counterfeit Clothing, 34
 - Counterfeit Banknotes, 34
 - Drug Trafficking, 35-41
 - Opium/Heroin/Morphine, 37
 - Amphetamine Type Stimulants (ATS), 38
 - Cocaine, 38-39
 - Cannabis, 40
 - Heroin, 40
 - Cocaine, 40
 - Black Market Peso Exchange, 41
 - Amphetamine Type Stimulants (ATS), 41
- Environmental Crime, 42-47
- Deforestation, 43
- Mountaintop Removal Mining, 43
- Overfishing, 44
- CFCs/ODs, 44
- Oil and Gas, 45
- Waste Disposal, 46
- Chemicals, 46
- Oceans and Seas, 46
- Livestock, 47
- Shipping, 47
- Retailing, 47
- Nuclear, 47
- Extortion, 48-49
- Forgery, 50-51
- Fraud incl Tax Fraud & Cybercrime, 52-62
- Accounting Fraud Schemes, 53

--Rogue/Unauthorised Trading, 54
--Hedge Fund/Investment Company Fraud, 55
--Boiler Rooms, 56
--Prime Bank Instruments/Schemes, 56
--Investment Frauds, 56-57
--Investment/Ponzi Schemes, 56
--The Pyramid Scheme, 57
--Nigerian Letter (419)/Advance Fee/Lottery Frauds, 57
--Advance Fee Frauds, 57
--Disaster Fraud, 57
--Foreign Lottery Fraud, 57
--Overpayment Fraud, 57
--Recovery Schemes, 57
--Banking/Payment Card Fraud, 58
--PB Fraud/Broker Embezzlement, 58
--Credit & Debit Card Fraud (including Counterfeit Cards), 58
--Cheque Kiting, 58
--Identity Theft/Bank Account Takeover, 58
--Mortgage and other Credit/Loan Frauds, 58
--Trade Based Money Laundering, 59
--Under Invoicing/Over Invoicing, 59
--Countering Trade Based Money Laundering, 59
--Tax Evasion/Tax Fraud, 60
--MTIC/Carousel Fraud, 60
--Cybercrime, 61
--Cyber Terrorism, 61
--Organised Crime, 61
--Human Trafficking, 63-65
--Illicit Arms Trafficking, 66-68
--Insider Dealing, 69-77
--Misuse of Information, 77
--Front/Parallel Running, 77
--Kidnap, Illegal Restraint & Hostage Taking, 78-81
--Market Manipulation, 82-88
--Abusive Rate Fixings/(Intimidation/Co-ordination), 83
--Abusive Short Selling, 84
--Abusive Squeezes, 84
--Amends, 84
--Backing Away, 84
--Banging the Close, 84
--Bear Raids, 84
--Best Execution, 84
--Bucketing, 84
--Bucket Shop, 84
--Cancellations, 84
--Capping, 84
--Cherry Picking, 84
--Churning, 84
--Circular Trading, 84
--Cornering, 84
--Crossing Trades, 84
--Curb Trading, 84
--Directed Trading, 84
--Fictitious Orders, 85
--Front Running, 85

--Ginzy Trading, 85
--Hack Pump & Dump, 85
--Insider Dealing/Trading, 85
--Inter-positioning, 85
--Intimidation/Co-ordination, 85
--Laddering, 85
--Large and Unusual Orders, 85
--Late Trading, 85
--Layering, 85
--Excessive Mark-ups, 85
--Marking the Close, 85
--Marking the Open, 85
--Matched Order, 85
--Momentum Ignition, 86
--Naked Short Selling, 86
--Painting the Tape, 86
--Parking, 86
--Penny Stocks, 86
--Phantom Orders, 86
--Piggy Backing, 86
--Ping Orders, 86
--Ponzi Schemes, 86
--Portfolio Pumping, 86
--Pre-arranged Trading, 86
--Puffing, 86
--Pump & Dump, 86
--Quid Pro Quo Arrangements, 87
--Quote Stuffing, 87
--Ramping, 87
--Rumouring, 87
--Scalping, 87
--Selective Issuer Disclosure, 87
--Short & Distort, 87
--Snake Trading, 87
--Soft Dollar Arrangements, 87
--Spinning, 87
--Spoofing, 87
--Trade Shredding, 87
--Trash & Cash, 87
--Tailgating, 87
--Tipping, 87
--Uauthorised Trades, 87
--Unsuitable Trades, 88
--Unusual Order Price, 88
--Warehousing, 88
--Wash Trades, 88
--Vulnerable Markets and Notable Cases, 88
--Murder & Grievous Bodily Harm, 89-92
--Organised Crime, 93-99
--Africa, 95
--Middle East, 95
--Golden Crescent, 95
--India/Pakistan, 95
--Asia, 95
--Golden Triangle, 95

- China, 95
- Japan, 96
- Americas, 96
- United States of America, 96
- Mexico, 97
- Caribbean, 98
- Jamaica, 98
- Central America, 98
- South America, 98
- Brazil, 98
- Colombia, 98
- Venezuela, 99
- Eastern Europe, 99
- Western Europe, 99
- Smuggling, 100-105
- Gas & Oil, 100
- Cigarettes, 100
- Wildlife Smuggling & Poaching, 100
- Alcohol, 101
- Metals & Minerals, 101
- Goods, 102
- Gas & Oil Smuggling, 102
- Cigarette Smuggling, 103
- Wildlife Smuggling & Poaching, 103
- Alcohol Smuggling, 103
- Precious Metals & Stones Smuggling, 103
- Human Smuggling, 103
- Arms Smuggling, 103
- Cash Smuggling, 103
- Black Market Peso Exchange (BMPE), 105
- Terrorism Finance, 106-117
- Theft, Robbery and Trafficking, 118-122
- WMD Proliferation Finance, 123-126

Section 2 - Sub-section 1 - Money Laundering Risks

- Money Laundering Risks Identified, 131-135
- Financial Action Task Force/FATF, 131
- United States, 133
- European Union, 134
- Other Countries, 134
- The Wolfsberg Group, 134
- Additional Sources, 135

Section 2 - Sub-section 2 - Customer Risks

- Arms Dealers, 139-140
- Banks & other Financial Institutions, 141-142
- Cash Intensive Businesses, 143-144
- Retail Type Outlets, 143
- Private Automated Teller Machines (ATMs), 144
- Bulk Cash Shipments, 144
- Casino's including Internet Gambling, 145-151
- Significant Growth and Emerging Markets, 147
- Illegal Casino's and Gambling, 147
- High Seas Casino's, 147
- Junkets, 148

- VIP Rooms, 149
- Internet Gambling, 150
- Charities & Not For Profit Organisations, 152-153
- Gatekeepers, 154-156
- Offshore Companies, 155
- Foundations including Anstalts and Stiftungs, 156
- High Value Goods Dealers, 157-160
- Auctions, 158
- Art, 158
- Jewels & Real Estate, 158
- Planes, Automobiles and Yachts, 158
- Animals, 159
- Watches, 160
- Wine and Champagne, 160
- Intermediaries, 161
- Money Services Businesses, 162-165
- Unregulated Money Service Businesses (UMSB), 164
- Chop, 165
- Fei' ch'ien, 165
- Hawala, 165
- Hundi, 165
- Politically Exposed Persons, 166-168
- Sovereign Wealth Funds, 168
- Precious Metals & Stones Dealers, 169-172
- Digital Precious Metals, 171
- Conflict Diamonds or Blood Diamonds, 171
- Angola, 171
- Liberia & Sierra Leone, 171
- Ivory Coast, 172
- Democratic Republic of the Congo, 172
- The Republic of Congo, 172
- Zimbabwe, 172
- Kimberley Process Certification Scheme (KPCS), 172
- Private Military Firms, 173-174
- Real Estate Agents, 175/176

Section 2 - Sub-section 3 - Products & Services (incl Channels) Risks

- A Brief History of Banking, 179-180
- Asset Management, 181-182
- Sensitive Customers, 182
- Customers with Material Sensitive Country Risk Exposure, 182
- Politically Exposed Persons, 182
- Charities of other Not for Profit Organisations, 182
- Sanctioned or Otherwise Problematic Customers, 182
- Fraud, 182
- Employee/Market Abuse, 182
- Brokerage/Securities, 183-185
- Customers with Cash Businesses, 184
- Customers with Sensitive Businesses, 184
- Customers with Material Sensitive Country Risk Exposures, 184
- Complex or Complicated Non-Transparent Customers, 185
- Politically Exposed Persons, 185
- Sanctioned or Otherwise Problematic Customers, 185
- Fraud including Market Abuse, 185
- Tax Evasion, 185

- Employees, 185
- Customers with Physical or Bearer Securities, 185
- Commercial Banking, 186-190
- Trade Finance, 186
- Customers with Cash Businesses, 189
- Customers with Sensitive Businesses, 189
- Businesses with Material Sensitive Country Risk Exposures, 189
- Politically Exposed Persons, 189
- Charities or other Not for Profit Organisations, 189
- Sanctioned or Otherwise Problematic Customers, 189
- Corruption Slush Funds, 190
- MTIC/Carousel and/or Tax Frauds, 190
- Trade Based Money Laundering including Trade Finance, 190
- Fraud, 190
- Correspondent Banking, 191-197
- Shell Bank Customers or Banks with Shell Banks as Customers, 193
- Offshore Banks, 194
- Non-Bank Financial Institutions (for example MSBs), 194
- Customers with Material Sensitive Country/PEP Risk Exposures, 194
- Sanctioned or Otherwise Problematic Customers, 194
- Group Companies, Parents, Subs and Affiliates, 194
- Wire Transfers, 194
- Payable Through Accounts (PTA), 196
- Pouch Services, 197
- Downstream Clearing/Nested Accounts, 197
- Banknote/Precious Metals Services, 197
- Credit & Other Cards, 198-200
- Top ML Risks/Credit & Debit Card Fraud, 200
- Investment Banking, 201-204
- Rogue/Unauthorised Traders, 203
- Insider Dealing by Employees, 203
- Market Manipulation by Employees, 203
- Bribery by Employees, 203
- Market Abuse by Customers, 204
- Sensitive Customers, 204
- Customers with Material Sensitive Country Risk Exposures, 204
- Politically Exposed Persons, 204
- Sanctioned or Otherwise Problematic Customers, 204
- High Frequency/Algo Trading and Dark Pools, 204
- Retail Banking, 205-208
- Customers with Cash Transactions, 206
- Customers with Material Sensitive Country Risk Exposures, 206
- Complex or Complicated Non-Transparent Customers, 206
- Sanctioned or Otherwise Problematic Customers, 207
- Credit and Loan Fraud, 207
- Identity Theft and Account Takeover, 207
- Tax Evasion, 207
- Credit Card and other Card Fraud, 207
- Bank Robbery, 207
- New Payment Methods, 207
- Wealth Management/Private Banking, 209-212
- Customers with Cash Transactions, 211
- Customers with Cash Businesses, 211
- Customers with Sensitive Businesses, 212
- Customers with Material Sensitive Country Risk Exposures, 212

- Complex or Complicated Non-Transparent Customers, 212
- Politically Exposed Persons, 212
- Sanctioned or Otherwise Problematic Customers, 212
- Fraud including Market Abuse, 212
- Tax Evasion, 212
- Employees, 212

Section 2 - Sub-section 4 - Country Risks

- Country Risks Methodology & Sources, 215-221
- Financial Action Task Force, 215
- High-Risk and Non-Cooperative Jurisdictions, 215
- Public Statement February 2013, 216
- Public Statement February 2013, 216
- Sanctioned Countries, 216
- United Nations, 216
- European Union (EU), 217
- US/OFAC, 217
- Switzerland/SECO, 217
- Others, 217
- Wolfsberg Group, 217
- Basel Institute of Governance, 218
- Additional Country Sources, 218
- Bertelsmann Stiftung's Transformation Index (BTI), 219
- Control Risks - Risk Module including Political, Operational, Security and Terrorism Rating, 219
- Egmont Group, 219
- Euromoney Country Risk Rating, 219
- EU - Common Understanding of the Procedure on Criteria for the Recognition of Third Countries' Equivalence agreed by Member States, 219
- Freedom House - Freedom in the World, 219
- OECD, International Tax Standards, 220
- Transparency International Corruption Perceptions Index (TI CPI), 220
- Transparency International - Global Corruption Barometer, 220
- US Department of State Country Report of Terrorism - supporters of International Terrorism (Bureau of Counter Terrorism), 220
- US Department of State - International Narcotics Control Strategy Report (INCSR), 220
- US State Department - Trafficking in Persons Report 2010 (TIP) including Human Trafficking Tier Lists, 220
- Fund for Peace (FFP) - The Failed States Index (2012) - The US think-tank, 220
- The World Bank Group - Worldwide Governance Indicators (WGI), 220
- The World Bank Group - Ease of Doing Business Index 2012, 221
- Further Resources, 221
- KnowYourCountry.com, 221
- Hot Spots (in-Country and Regional), 221
- Diversion Risk or Close Proximity Risk, 221
- Free Trade Zones, 222
- Time Zone Risk, 222

Section 3 - Money Laundering Laws & Regulations

- Introduction, 225

AML Treaties, Conventions & Major Laws, 228-246

- 1912 - The International Opium Convention (the "Hague Convention"), 226
- 1925 - The International Opium Convention (the "Geneva Convention"), 226
- 1925 - The Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare (the "Geneva Protocol"), 226
- 1933 - The USA Securities Act, 226

--1933 - USA Banking Act (Glass-Steagall Act), 226
--1934 - USA Securities & Exchange Act, 226
--1936 - The USA Commodity Exchange Act, 226
--1942 - USA Exchange Act Rule 10b-5, 227
--1961 - Single Convention on Narcotic Drugs (amended by 1972 Protocol), 227
--1969 - Convention on Offences and Certain Other Acts Committed On Board Aircraft (the "Tokyo Convention"), 227
--1970 - USA/Organised Crime Control Act, 227
--1970 - Nuclear Non-Proliferation Treaty, 227
--1970 - USA - Bank Secrecy Act, 227
--1971 - Convention for the Suppression of Unlawful Seizure of Aircraft (the "Hague Convention"), 227
--1971 - Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (the "Montreal Convention"), 227
--1971 - Convention on Psychotropic Substances, 228
--1972 - The Biological Weapons Convention, 228
--1973 - Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, 228
--1975 - Convention on International Trade in Endangered Species of Wild Flora and Fauna (CITES or the "Washington Convention"), 228
--1977 - Switzerland - The agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB) (revised latest 2008), 228
--1977 - USA Foreign Corrupt Practices Act (FCPA), 228
--1983 - International Convention against the Taking of Hostages (The "Hostage Convention"), 228
--1984 - USA - Insider Trading Sanctions Act, 228
--1985 - UK Company Securities (Insider Dealing) Act, 229
--1986 - USA - Money Laundering Control Act, 229
--1987 - Convention on the Physical Protection of Nuclear Material (CPPNM), 229
--1988 - Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 229
--1988 - BIS - Basel Committee on Banking Supervision Prevention of Criminal use of the Banking System for the purposes of Money Laundering, 229
--1988 - UN Convention against illicit trafficking in narcotic drugs and psychotropic substances (the "Vienna Convention"), 229
--1989 - European Community Directive Coordinating Regulations on Insider Trading, 230
--1990 - FATF 40 Recommendations First Issue, 230
--1991 EU First Money Laundering Directive, 230
--1992 - Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 230
--1993 - Convention on Biological Diversity (CBD), 230
--1993 - The Chemical Weapons Convention, 231
--1996 - USA Inter-American Convention against Corruption, 231
--1996 - FATF 40 Recommendations - Revised, 231
--1997 - International Convention for the Suppression of Terrorist Bombings (Terrorist Bombings Convention), 231
--1998 - UN Political Declaration and Action Plan against Money Laundering, 231
--1998 - EU Council of Europe Criminal Law Convention & Civil Law Convention, 231
--1998 - BIS - Basel Committee on Banking Supervision - "Prevention of criminal use of the banking system for the purpose of money laundering", 232
--1999 - OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, 232
--1999 - International Convention for the Suppression of the Financing of Terrorism ("The Terrorist Financing Convention"), 232
--1999 - USA Financial Services Modernisation Act Gramm-Leach-Bliley, 232
--2001 - Convention against Transnational Organised Crime (the "Palermo" Convention), 232
--2001 - EU Second Money Laundering Directive, 232

--2001 - BIS - Basel Committee on Banking Supervision its Customer Due Diligence Paper for Banks, 233
--2001 - USA - Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act (the "PATRIOT" Act), 233
--2001 - FATF 8 Special Recommendations on Terrorism Finance (later to be become 9 Special Recommendations in 2004), 233
--2002 - USA - Act to Protect Investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes; also known as "Public Company Accounting Reform and Investor Protection Act" and "Corporate and Auditing Accountability and Responsibility Act" but more commonly known as "Sarbanes Oxley" or "SOX", 233
--2003 - FATF 40+8 Recommendations - Revised, 234
--2003 - UN Convention against Corruption (UNCAC), 234
--2003 - The Trafficking in Persons Protocol Palermo Protocol (Protocol to the Convention against Transnational Organised Crime 2000), 234
--2003 - African Union Convention on Preventing and Combating Corruption, 234
--2003 - BIS - Basel Committee on Banking Supervision issued a General Guide to account opening and customer identification, 235
--2004 - The Smuggling of Migrants by Land, Sea and Air - Palermo Protocol (Protocol to the Convention against Transnational Organised Crime 2000), 235
--2004 - BIS - Basel Committee on Banking Supervision issued its "Consolidated KYC Risk Management", 235
--2005 - EU Market Abuse Directive ("MAD"), 235
--2005 - EU Third Money Laundering Directive, 235
--2005 - Protocol against the Illicit Manufacturing and Trafficking in Firearms, Their Parts and Components and Ammunition - Palermo Protocol (Protocol to the Convention against Transnational Organised Crime 2000), 236
--2005 - Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 236
--2006 - US Unlawful Internet Gamblin Enforcement Act (UIGEA), 236
--2008 - Switzerland- Market Conduct Rules - FINMA Circular, 236
--2009 - UK - FSA Code of Market Conduct, 236
--2009 - OECD Recommendations for Further Combating Bribery of Foreign Public Officials in International Business Transactions, 237
--2010 - USA - The Foreign Account Tax Compliance Act (FATCA), 237
--2010 - UK - Bribery Act, 237
--2010 - Convention on Cluster Munitions (CCM), 237
--2010 - USA - The Dodd-Frank Wall Street Reform Act, 237
--2011 - EU - Second Market Abuse Directive ("MAD 2") - Proposals, 238
--2012 - FATF 40 Recommendations (International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation), 239
--2012 - Switzerland - Stock Exchange Act (Amended), 239
--2012 - EU 4th AML Directive - Proposed and Funds Transfer Regulations Proposed, 240
--2012 - EU - Directive on Freezing and Confiscation of The Proceeds of Crime -Proposed, 241
--2012 - USA - Advance Notice of Proposed Rulemaking on Customer Due Diligence (Expanding BO ID requirements) - Proposed, 241
--2013 - Switzerland - Federal Act on War Materials, 243
--2013 - Switzerland - Money Laundering Act - Proposed implementation of (a) FATF recommendations and (b) Financial Market Strategy, 243
--2013 - UN - The Arms Trade Treaty (ATT), 244
--2013 - Singapore - Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, 244
--2013 - BIS - Basel Committee on Banking Supervision - "Sound management of risks related to money laundering and financing of terrorism" - consultative document, 244

-Financial Action Task Force / FATF, 245-258

--2013 International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6), 245
--2013 Guidance on Politically Exposed Persons (Recommendations 12 and 22); 245
--2013 Guidance: The Implementation of Financial Provisions of UN Security Council Resolutions to Counter the

Proliferation of Weapons of Mass Destruction, 245
---2013 Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, 245
---2013 Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, 245
---2012 - International standards on combatting money laundering and the financing of terrorism and proliferation - revised 40 Recommendations., 247
---2012 Money Laundering and Terrorist Financing vulnerabilities of the illicit tobacco trade, 256
---2012 Specific Risk Factors in the Laundering of Proceeds of Corruption - Assistance to reporting institutions, 257
---2011 Laundering the Proceeds of Corruption, 257
---2011 Organised Maritime Piracy and Related Kidnapping for Ransom", 257
---2011 Money Laundering Risks Arising from Trafficking of Human Beings and Smuggling of Migrants, 257
---2010 Money Laundering Using Trust and Company Service Providers, 257
---2010 Money Laundering Using New Payment Methods, 257
---2010 Global Money Laundering & Terrorist Financing Threat Assessment, 257
---2010 Money Laundering through Money Remittance and Currency Exchange Providers, 257
---2010 Money Laundering vulnerabilities of Free Trade Zones, 257
---2009 Money Laundering and Terrorist Financing in the Securities Sector, 257
---2009 Money Laundering through the Football Sector, 257
---2009 Vulnerabilities of Casinos and Gaming Sector, 257
---2008 Typologies Report on Proliferation Financing, 257
---2008 Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems, 257
---2008 Money Laundering & Terrorist Financing Risk Assessment Strategies and Terrorist Financing Typologies, 257
---2007 Money Laundering and Terrorist Financing Through the Real Estate Sector, 258
---2007 Laundering the Proceeds of VAT Carousel Fraud Report, 258
---2007 The Misuse of Corporate Vehicles, Including Trust and Company Service Providers, 258
---2006 Report on New Payment Methods, 258
---2006 Trade-Based Money Laundering, 258
---2004 The Abuse of Alternative Remittance Systems (SR VI) Best Practice, alternative remittance, 258
---2004 Best Practice, cash couriers, bearer negotiable instruments, SR IX, 258
---2003 Third revision of its 40/8 Recommendations, 258
---2002 International Best Practices: Combating the Abuse of Non-Profit Organisations (SR VIII), 258
---2002 Guidance for financial institutions in detecting terrorist financing, 258
---2001 Issue of 8 Special Recommendations on Terrorist Financing, 258
---2001 Typologies on Behind the Corporate Veil, 258
---1996 First revision of 40 Recommendations and issues its first typology report, 258
---1990 FATF issued its 40 Recommendations, 258

-Wolfsberg Group AML Standards & Work, 259-263

---The Anti-Money Laundering (AML) Principles 2000 / Global AML Guidelines for Private Banking 2002 (first revision), 259
---Statement Against Terrorist Financing 2002, 260
---Correspondent Banking Principles 2002, 260
---Statement on Monitoring Screening and Searching 2003, 260
---Launch of the Bankers Almanac Due Diligence Registry 2004, 260
---Correspondent Banking FAQ's 2006, 260
---Guidance for Mutual Funds and Other Pooled Investment Vehicles 2006, 261
---Investment and Commercial Banking FAQs 2006, 261
---Guidance on a Risk Based Approach 2006, 261
---Statement against Corruption Guidance 2007, 261
---Transparency of International Wire Transfers 2007, 261
---FAQs on PEPs revised and reissued 2008, 261

---Statement on Monitoring, Screening & Searching revised and reissued 2009, 262
---Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities 2009, 262
---Wolfsberg Anti-Corruption Guidance 2011, 262
---Trade Finance Principles 2009 and 2011, 262
---Guidance on Prepaid and Stored Value Cards 2011, 262
---Private Banking Principles 2012, 263
---FAQs on Intermediaries 2012, 263
---Beneficial Ownership FAQs 2012, 263
---The Wolfsberg Forum, 263
---The Wolfsberg AML Risk Radar 2013, 263

-Sanctions & Embargoes, 264-279

---Terrorism, 264
---9/11 - Attacks on America, 265
---Reforms, 265
---US Anti-Terrorism Programme, 265
---9/11 Litigation Cases, 266
---Drug Trafficking, 267
---Cali Executive Order 12978, 267
---Weapons of Mass Destruction, 267
---Country Sanction Programmes, 268
---Belarus, 268
---Democratic Republic of the Congo, 269
---The First Congo War (1996), 269
---The Second Congo War (1998), 269
---Cuba, 270
---Palestinian Territories, 270
---Linde v. Arab Bank, 270
---Rothstein v. UBS, 271
---Weiss v National Westminster Bank, 271
---Strauss v. Crédit Lyonnais, 272
---Keren Elmaliah v. Bank of China Ltd, 272
---Gill v. Arab Bank, 272
---Iran, 272
---US Sanctions, 273
---Nuclear Threat and Multilateral Sanctions, 273
---Myanmar, 275
---North Korea, 276
---Sudan, 277
---Syria, 277
---Venezuela, 279
---Zimbabwe, 279

Section 4 - Money Laundering Prevention Programmes

--Risk Based Approach, 283-284
--Risk Assessment, 285-294
---The Purpose of a Risk Assessment, 285
---Frequency of Assessment and Periodic Updates, 286
---Ownership, Roles & Responsibilities, 286
---AML/Sanctions/Anti-Bribery & Corruption (ABC), 286
---Conventional/Standard AML, Risk Assessment Model, 286
---Phase 1 - Inherent Risk Assessment, 287-290
---Clients Risk, 287
---Products and Services Risk, 288
---Channels Risk, 288

- Geography/Country Risk, 289
- Other Qualitative Risk Factors, 289
- Standardised Industry Inherent Risk Ratings, 290
- Phase 2 - Assessment of Internal Controls, 290-291
- Legal/Compliance/AML Unit Override, 290
- Phase 3 - Arriving at the Net - Residual Risk, 291
- Low Residual Risk, 291
- Moderate Residual Risk, 291
- High Residual Risk, 291
- Reporting & Communication of Results, 291
- Note on Links to Customer Risk Rating Models, 291
- Note on Links to Risk Based Approach, 291
- Other Approaches - Scenario Based Approach, 292-294
- Part 1 - Build the Scenarios, 293
- Part 2 - Score the Scenarios, 293
- Part 3 - Determine the Inherent Risk, 293
- Risk Assessment and Risk Appetite, 294

--AML Programme, 295-300

- Policies, Procedures and Controls, 296
- Customer Identification Programme, 297
- Detection and SAR Filing, 297
- Risk Assessment, 297
- Monitoring and Controls, 298
- MIS/Reporting, 299
- Record Keeping, 299
- Designated Compliance Officer, 299
- Training Programme, 300
- Independent Testing, 300

--Sanctions Programme, 301-305

- Policies, Procedures and Controls, 301
- Sanctions Compliance Policy, 301
- Detection and SAR Filing, 302
- Risk Assessment, 302
- Monitoring and Controls, 302
- International Fund Transfers, 302
- Correspondent Banking, 303
- International commercial shipping lines or freight forwarders operating via transit routes known for drugs, arms or sanctioned parties, 303
- Energy and Commodities companies operating in sanctioned regions, 304
- Money Service Businesses, 304
- Charities, 304
- MIS/Reporting, 304
- Record Keeping, 305
- Designated Compliance Officer, 305
- Training Programme, 305
- Independent Testing, 305

--Anti-Bribery & Corruption Programme, 306-309

- Policies, Procedures and Controls, 306
- Code of Conduct/Specific Policies, 306
- Detection and SAR Filing, 306
- Risk Assessment, 306
- Monitoring and Controls, 306

- Public Officials, 307
- Dealing with persons from jurisdictions or in industries with inherent elevated risks of corruption, 307
- Gifts, hospitality, entertainment and travel, 307
- Political contributions, 307
- Charitable donations and sponsorships, 307
- Facilitation payments, 307
- Books and records, 308
- Solicitations, 308
- Offers of employment, internships, 308
- Dealings with third parties, agents and intermediaries, 308
- MIS/Reporting, 308
- Record Keeping, 308
- Designated Compliance Officer, 309
- Training Programme, 309
- Independent Testing, 309

--Anti-Fraud Programme, 310-314

- Policies, Procedures and Controls, 310
- Code of Conduct/Specific Policies, 310
- Detection and SAR Filing, 310
- Behavioural Red Flags, 311
- Risk Assessment, 311
- Monitoring and Controls, 311
- Segregation of duties, 311
- Internal fraud, 311
- External fraud or theft, 311
- IT governance, 312
- Procurement, 312
- Human Resources, 312
- Finance, 313
- Whistleblowing, 313
- MIS/Reporting, 313
- Record Keeping, 314
- Designated Officer, 314
- Training Programme, 314
- Independent Testing, 314

Part 2

Section 5 - Regions, Countries, Criminals & Terrorists

- Introduction, 319-320
- UN Designated Terrorist Organisations, 320
- Africa, 321-346
- North Africa, 322-325
- Algeria, 322
- Armed Islamic Group, 322
- Western Sahara, 323
- Mauritania, 323
- Libya, 323
- Libyan Islamic Fighting Group, 323
- Morocco, 324
- Moroccan Islamic Combatant Group, 324
- Tunisia, 324
- Tunisian Combatant Group, 324

- Al-Qaeda in the Islamic Maghreb, 325
- West Africa, 326-329
 - Nigeria, 326
 - Nigerian Crime Gangs, 327
 - Movement for the Emancipation of the Niger Delta, 327
 - Boko Haram, 338
 - Area Boys - Agberos, 328
 - Sierra Leone, 328
 - Revolutionary United Front, 329
 - Liberia, 329
 - Mali, 329
 - Ansar Dine, 329
- The Horn of Africa, 330-331
 - Djibouti, 330
 - Eritrea, 330
 - Ethiopia, 330
 - Somalia, 331
 - Al-Shabaab, 331
- Eastern Africa, 332-336
 - Sudan, 332
 - South Sudan, 333
 - Sudan People's Liberation Army, 333
 - Uganda, 333
 - Lord's Resistance Army, 334
 - Kenya, 335
 - Mungiki, 335
 - Tanzania, 336
 - Madagascar, 336
- Central Africa, 337-340
 - Rwanda, 337
 - Army for the Liberation of Rwanda, 337
 - Rwandan Patriotic Army, 338
 - Democratic Republic of the Congo, 338
 - Republic of the Congo/Congo Brazzaville, 339
 - Gabon, 339
 - Central African Republic, 339
 - Chad, 339
 - Burundi, 340
 - Cameroon, 340
 - São Tomé and Príncipe, 340
 - Equatorial Guinea, 340
 - Southern Africa, 341-346
 - South Africa, 341
 - People Against Gangsterism and Drugs, 342
 - Numbers Gang, 343
 - Angola, 343
 - National Union for the Total Independence of Angola (UNITA), 343
 - Lesotho, 343
 - Namibia, 344
 - Mozambique, 344
 - Mozambique National Resistance Movement (RENAMO), 344
 - Botswana, 345
 - Swaziland, 345
 - Zimbabwe, 345
 - Zambia, 346
 - Middle East, 347-365
 - Israel/Palestine, 347
 - Irgun, 349
 - Kahane Chai, 349
 - Abergil Crime Family, 349
 - Alperon Crime Family, 349
 - Zeev Rosenstein Organisation, 349
 - Palestine Liberation Organsaiton, 349
 - Fatah, 350
 - Al-Aqsa Martyrs' Brigade, 350
 - Tanzim, 350
 - Black Septemeber, 351
 - Abu Nidal Organisation, 351
 - Popular Front for the Liberation of Palestine, 352
 - Democratic Front for the Liberation of Palestine, 352
 - Palestine Islamic Jihad, 352
 - Palestine Liberation Front, 353
 - Army of Islam, 353
 - Hizb ut-Tahrir, 353
 - Hamas - Palestine, 354
 - Syria, 355
 - Syrian Islamic Liberation Front, 355
 - Syrian Islamic Front, 355
 - Al-Nusra Front/Jubhat al Nusra, 355
 - The Islamic State of Iraq and Syria, 355
 - Lebanon, 356
 - Jund al-Sham, 356
 - Amal, 356
 - Asbat al-Ansar, 356
 - Hezbollah - Lebanon, 357
 - Iraq, 358
 - Al-Qaeda in Iraq, 359
 - Abdullah Azzam Shaheed Brigades, 360
 - Ansar Al-Islam, 360
 - Jamaat Ansar al-Sunna, 360
 - Khata'ib Hezbollah, 360
 - Iran, 361
 - Islamic Revolutionary Guards, 362
 - Mujahadin-e Khalq, 362
 - Jundallah, 362
 - Gulf States, 363
 - United Arab Emirates, 363
 - Saudi Arabia, 363
 - Yemen, 364
 - Al-Qaeda in the Arabian Peninsula, 365
 - Ansar al-Sharia, 365
 - Egypt, 366
 - Muslim Brotherhood, 366
 - Egyptian Islamic Jihad, 366

- Gama'a al-Islamiya, 367
- Turkey, 368
- Turkey Designated Terrorist Organisations, 368
- Kurdistan Workers Party, 368
- Kurdistan Freedom Falcons, 369
- Revolutionary Peoples Liberation Party-Front, 369
- Turkish Mafia, 369
- Ulkuçu Hareket, 369
- Asia, 370-416
 - Southern Asia, 370-396
 - Afghanistan, 371
 - Al-Qaeda, 372
 - Afridi Network, 376
 - Taliban - Afghanistan, 377
 - Noorzai Organisation, 378
 - Khan Cartel, 378
 - Pakistan, 379
 - Hizb-e-Islami Gulbuddin, 379
 - Jamiat-e-Islami, 380
 - Quetta Shura, 380
 - Tehrik-Taliban/Pakistan Taliban, 380
 - Haqqani Network, 380
 - Tahreek-e-Nafaz-e-Shariat-e-Mohammadi, 381
 - Lashkar I Jhangvi, 381
 - Islamic Jihad Union, 382
 - Sipah-e-Sahaba, 382
 - Kashmir, 382
 - Lashkar-e-Tayyiba (LeT), 383
 - Jaish-e-Mohammed (JEM), 384
 - Harakat-ul Jihad Islami (HUJI), 384
 - Harakat ul-Mujahideen (HUM). 384
 - Al-Umar Mujahideen, 385
 - Dukhtaran-e-Millat, 385
 - Hizb ul-Mujahideen, 385
 - Balochistan Liberation Army, 385
 - India, 386
 - Indian List of Designated Terrorist Organisations, 386
 - Indian Gangs, 387
 - D-Company, 387
 - Students Islamic Movement of India, 387
 - Indian Mujahideen (IM), 388
 - Sikh Terrorism, 388
 - Babbar Khalsa International, 388
 - Deendar Anjuman, 388
 - North Eastern India, 388
 - Kanglei Yawol Kanna Lup, 389
 - People's Liberation Front, 389
 - Revolutionary People's Front of Manipur, 389
 - People's Revolutionary Party of Kangleipak, 389
 - United National Liberation Front, 389
 - United Liberation Front of Asom, 390
 - National Democratic Front of Bodoland, 390
 - National Liberation Front of Tripura, 390
 - Garo National Liberation Army, 391
 - Hynniewtrep National Liberation Council (HNLC) Meghalaya-Garoland, 391
 - Achik National Volunteer Council (ANVC) - Garoland, 391
 - Tamil Nadu Liberation Army, 391
 - Tamil National Retrieval Troops, 391
 - Communist Party of India (CPI-Maoist)/The Maoist Communist Centre of India (MCC), 392
 - Bangladesh, 392
 - Jamaat-ul-Mujahideen, 392
 - Harakat-ul-Jihad-Islami, 393
 - Nepal, 393
 - The Communist Party of Nepal-Maoist, 393
 - Akhil Bharat Nepali Ekta Samaj, 394
 - Sri Lanka, 394
 - Liberation Tigers of Tamil Eelam, 395
 - World Tamil Movement, 396
 - Tamil Rehabilitation Organisation, 396
 - South East Asia, 397-403
 - Indonesia. 397
 - Jemmah Islamiya, 397
 - Jemmah Anshorut Tauhid, 398
 - Free Papua Movement, 398
 - Malaysia, 398
 - Philippines, 399
 - Abu Sayyaf, 399
 - New People's Army, 400
 - The Moro Islamic Liberation Front, 400
 - Rajah Solaiman Movement, 401
 - Vietnam, 401
 - Golden Triangle Cartels, 401
 - Thailand, 402
 - Jao/Chao Pho, 402
 - Laos, 402
 - Myanmar, 403
 - Khun Sa Cartel, 403
 - United Wa State Army/Red Wa, 403
 - Eastern Asia, 404-413
 - China, 404
 - China Designated Terrorist Organisations, 405
 - World Uyghur Youth Congress, 405
 - The Eastern Turkistan Islamic Movement, 406
 - Chinese Black Societies,, 406
 - Tongs, 406
 - Triads, 407
 - Sun Yee On, 407
 - 14K, 407
 - Dai Huen Jai, 407
 - Taiwan, 408
 - Heijin, 408
 - United Bamboo, 408
 - Heavenly Alliance Gang, 408
 - Four Seas Gang, 408
 - North Korea, 409
 - South Korea, 409
 - Japan, 410
 - Japanese Red Army, 411

--Aum Shinrikyo, 411
--Yakuza, 411
--Yamaguchi-gumi, 413
--Sumiyoshi-kai, 413
--Inagawa-kai, 413
--Dojin-kai, 413
--Kyushi Seido-kai, 413

-Central Asia, 414-416
--Uzbekistan, 415
---Islamic Movement of Uzbekistan, 415
---Islamic Jihad Group, 416
--Khazakhstan, 416

-Oceania, 417-418
--Australia, 417
---Designated Australian Terrorist Organisations, 418
-- New Zealand, 418
---Mongrel Mob, 418
--Pacific Islands, 418
--Vanuatu, 418

Americas, 419-468
-- United States, 420-431
---US Designated Terrorist Organisations, 420
---US Gangs, 420
---American Street Gangs, 421
---The Crips, 421
---The Bloods, 422
---Mara Salvatrucha -13, 423
---18th Street Gang, 423
---Latin Kings, 423
---Wah Ching, 424
---Black Guerrilla Family (Black Family, Black Vanguard), 425
---American Prison Gangs, 425
---The Aryan Brotherhood, 425
---Mexican Mafia (La eMe), 425
---La Nuestra Familia, 425
---Texas Syndicate (Texas 7), 426
---Ku Klux Klan, 426
---Weathermen/Weather Underground, 426
---American Mafia, 427
---Outlaw Motorcycle Gangs, 429
---Hell's Angels, 430
---The Bandidos, 431
---The Outlaws, 431
---The Pagans, 431
---The Mongols, 431
---The Vagos Motorcycle Club, 431
---Wheels of Soul, 431
--Canada, 432-434
---Canadian Designated Terrorist Organisations, 434
--Mexico, 435-442
---Mexican Drug Trafficking Organisations (DTOs), 437
---The Leading Mexican Cartels, 440

--Gulf Cartel, 440
--Juarez Cartel, 441
---Sinaloa Cartel, 441
---Tijuana Cartel, 441
---La Familia Michoacano (Disbanded), 441
---Knights Templar, 441
---Beltran Leyva Cartel (Disbanded), 442
---Los Zetas Cartel, 442
-Caribbean, 443-445
--Bahamas, 444
--Cuba, 444
--Dominican Republic, 444
--Jamaica, 445
---Yardies/Shower Posse, 444
--Haiti, 445

-Central America, 446-450
-- Northern Triangle, 446
---Mara - MS13/MS18, 447
--El Salvador, 448
---People's Liberation Forces, 448
---Farabundo Martin National Liberation Front (FMLN), 448
--Honduras, 449
--Guatemala, 449
--Panama, 449
--Nicaragua, 450
---Nicaraguan Democratic Force (Contras), 450
--Belize, 450
--Costa Rica, 450

-South America, 451-468
--Tri-Border Region, 451
--Brazil, 452
---Blue Command, 452
---Red Command, 453
---First Capital Command (PCC), 453
--Argentina, 453
---People's Revolutionary Army, 454
---Anti-Communist Alliance, 454
--Paraguay, 454
--Uruguay, 454
---Tupamaros, 455
--Ecuador, 455
--Bolivia, 455
---National Liberation Army, 456
--Chile, 456
---Movement of the Revolutionary Left (MIR), 456
---Manuel Rodriguez Patriotic Front, 456
--Peru, 457
---Shining Path, 457
---Tupac Amaru Revolutionary Movement (MRTA), 458
--Colombia, 459
---April 19 Movement (M-19), 459
---United Self Defence Forces of Colombia (AUC), 459
---FARC/The Revolutionary Armed Forces of Colombia, 460

--ELN/National Liberation Army, 460
--ERPAC /Popular Revolutionary Anti Terrorist Army of Colombia, 461
--The Aguilas Negras or Black Eagles, 461
--Colombian Drug Cartels, 462
--The Cali and Medillin Cartels, 462
--Oficina de Envigado, 465
--North Coast Cartel, 465
--Norte del Valle Cartel, 465
--Los Rostros, 466
--Urabenos, 466
--Venezuela, 466
--Cartel of the Suns, 467
--Walid Makled, 467
--The Bolivarian Liberation Forces, 467
--Guyana/French Guyana & Suriname, 468

Europe, 469-506
--Neo Nazism, 469

-Eastern Europe, 470-484
--Baltic States, 470
--Poland, 471
--Pruszkow Mafia, 471
--Bulgaria, 471
--Balkan's and Former Yugoslavia, 472
--Serbia, 472
--Serbian Mafia, 472
--Bosnia & Herzegovina, 473
--Bosnian Mujahideen, 473
--Kosovo, 473
--Kosovo Liberation Army, 474
--Albania, 474
--Albanian Mafia, 474
--Nano Aldo Bare, 475
--Belarus, 475
--Ukraine, 475
--Moldova, 476
--Hungary, 476
--Romania, 476
--Transcaucasus Region, 476
--Armenia, 477
--Azerbaijan, 477
--Georgia, 477
--Russia, 478
--Russian Designated Terrorist Organisations, 479
--Russian Mafia, 479
--Solntsevskaya Bratva, 480
--Tambov Syndicate, 480
--Semion Mogilevich, 480
--Ciscaucasus/North Caucasus, 481
--The Republic of Chechnya, 481
--The Islamic International Peacekeeping Brigade, 482
--Special Purpose Islamic Regiment, 482
--Riyad us-Saliheyn Martyrs' Brigade, 483
--Caucasus Emirate, 483

--Chechen Mafia, 484
--Obshina - Chechnya, 484
-Western Europe, 485-506
--European Union Designated Terrorist Organisations, 485
--Abu Hafs al-Masri Brigade, 485
--Bader Meinhof Group/Red Army Faction, 486
--Dutch Gangs - Netherlands, 486
--Bruinsma Drug Gang, 486
--Willem Holleeder Gang, 487
--Hofstad Network, 487
--Communist Combatant Cells, 487
--Original Gangsters, 487
--Uppsala Mafia, 487
--Black Cobra, 487
--Euskadi Ta Askatasuna (ETA), 488
--France, 490-492
--French Designated Terrorist Organisations, 490
--Corsican Mafia, 491
--Corsican Patriotic Front, 491
--Tractions Avant Gang, 491
--Hornec Gang, 491
--Mad Jacky Gang, 491
--Action Directe, 492
--Revolutionary Organisation 17th November, 492
--Revolutionary Struggle, 492
--Conspiracy of Fire Nuclei, 492
--Cyprus, 493
--Holy See (Vatican City), 493
--Italy, 493-495
--Red Brigades, 493
--Italian Mafia, 494
--La Cosa Nostra, 494
--Camorra Mafia, 495
--Ndrangheta Mafia, 495
--Sacra Corona Unita Mafia, 495
--United Kingdom-Ireland, 496-506
--United Kingdom list of Designated Terrorist Organisations, 496
--Saor Eire, 496
--The Kray Twins, 496
--Clerkenwell Crime Syndicate/A Team, 497
--Noonan Gang, 497
--Thomas McGraw, 498
--Curtis Warren, 498
--Cahill Gang, 498
--Gilligan Gang, 499
--Foley Gang, 499
--Terrorist Groups, 499
--Irish National Liberation Army, 499
--Provisional Irish Republican Army, 500
--Continuity Irish Republican Army (CIRA), 505
--Cumann na Mban, 505
--Real Irish Republican Army (RIRA), 505
--The 32 County Sovereignty Movement Movement, 505
--Ulster Defence Association/Ulster Volunteer Force, 506

---Fianna Eireann, 506

Section 6 - Terrorist Attacks

Introduction, 509-510

-Chronology of the Worlds Worst Terrorist Attacks over the last 100 years, 511-530

---1914: Archduke Franz Ferdinand assassination in Sarajevo by Serbian Nationalist, 511

---1920: Wall Street Bombing: US by Galleanists (Italian anarchists) (38), 511

---1921: bombing of Bolgard palace in Bessarabia (modern Moldova) (100), 511

---1925: bombing of cathedral in Sophia, Bulgaria by Communist Revolutionaries (160), 511

---1933: First 2 Airline Attacks (15) and (7), 511

---1946 King David Hotel Bombing: Israel (91): Irgun, Jewish Terrorists, 511

---1948: Ben Yehuda Street bombing: Mandatory Palestine, Jerusalem by Palestinian Terrorists (58), 511

---1948: Mahatma Gandhi assassination by Hindu Nationalist Extremists, 512

---1963: US President JF Kennedy assassination by Lee Harvey Oswald, 512

---1968: US Senator Robert F. Kennedy assassination by Sirhan Sirhan, 512

---1972: Israel's Lod airport attack by Japanese Red Army supported by the General Command of the Popular Front for the Liberation of Palestine (26), 512

---1972: Munich Olympics, Germany by Black September (19), 512

---1973: Spanish Prime Minister Luis Carrero Blanco by ETA, 513

---1974: The Birmingham pub bombings in UK by IRA (21), 513

---1978: Cinema Rex Arson in Abadan, Iran by Iranian Revolutionaries (477), 513

---1979: Hostage taking at Grand Mosque in Mecca, Saudi Arabia (includes 87 Islamic terrorists killed) (240), 513

---1979: Lord Mountbatten (Cousin of the Queen of England) in Ireland assassinated by IRA, 513

---1978: Italian Prime Minister Aldo Moro kidnapped and assassinated by Red Brigade, 513

---1979: US Embassy Hostage Crises, Tehran, Iran, 513

---1980 -The Iranian Embassy Siege, London, UK, 513

---1981: President Anwar Sadat of Egypt assassinated by Al Gamaa al-Islamiyya, 514

---1982 : First truck bombing attack in Tyre Lebanon by Hezbollah (102), 514

---1983: Truck bombings of US Marine and French barracks, Beirut, Lebanon by Hezbollah (301), 514

---1983: Harrods Department Store bombing in London, UK by IRA (6), 514

---1984: Margaret Thatcher, British Prime Minister attempted assassination by IRA (5), 514

---1984: Golden Temple Seizure, Amritsar, India by Sikh Terrorists (100), 514

---1984: Indira Gandhi, Indian Prime Minister assassinated by Sikh Terrorists, 514

---1985: Attack on crowds in Sri Lanka by Tamil Tigers (150), 514

---1985: Attack on Rome and Vienna airports simultaneously by Abu Nidal Organisation (15), 514

---1987: Bus attacks in Sri Lanka by Tamil Tigers (233), 515

---1990: Attack at mosques in Sri Lanka by Tamil Tigers (300), 515

---1991: Rajiv Gandhi Indian Prime Minister, by Tamil Tigers (15), 515

---1992: Gold Mohur Hotel, Aden, Yemen by Al-Qaeda (2), 515

---1992 Israeli Embassy in Buenos Aires, bombed by Hezbollah (29), 515

---1993: Ranasinghe Premadasa, Sri Lankan President assassinated by Tamil Tigers (15), 515

---1993: World Trade Centre bombing, US, New York City by Al-Qaeda (6), 515

---1993: 15 bombings in Bombay, India by D- Company (317), 515

---1994: Asociacion Mutual Israelita Argentina (AMIA), bombed in Buenos Aires, Argentina by Hezbollah (86), 515

---1995: Paris Metro bombing in Paris, France by GIA (8), 516

---1995: Truck bombing of federal building, in Oklahoma City, USA by Anti Government Terrorist (168), 516

---1995: Sarin subway station Attack, Tokyo by Aum Shinri-Kyu (12), 516

---1996: Hostage taking in Budennovsk, Russia, by Chechen Terrorists (143), 516

---1996: Khobar Towers bombing in Khobar Saudi Arabia by Al-Qaeda (19), 516

---1997/1998: Attack at Ben Talha, and elsewhere in Algeria by Armed Islamic Group (1000+), 516

---1998: US Embassy bombings in Kenya and Tanzania by Egyptian Islamic Group and AQ (303), 516

---1998: Colombian Army ambushed by FARC (62), 517

---1999: Apartment bombings in Moscow Russia by Chechen Terrorists (301), 517

---2000: Rizal Day bombings in Philippines on the Metro Manila by Jemaah Islamiyah (22), 517

---2000: USS Cole bombing, Yemen, Aden by Al-Qaeda in the Arabian Peninsula (19), 517

---2000/2004: Second Intifada Bombings by Palestinian Terrorists in Israel (622), 517

---2001: Attacks on America (9/11) by Al-Qaeda (2,997), 518

---2001: Attack on a train in Angola by UNITA (152), 520

---2002: Bali Bombings in Indonesia by Jemaah Islamiyah (202), 520

---2002: Theatre Hostage Crisis, Moscow, Russia by Chechen Terrorists (168), 520

---2003: Red Square bombing in Moscow, Russia by Chechen Terrorists (6), 520

---2003: Compound bombings in Riyadh, Saudi Arabia by AQ (35), 520

---2003: Bombings at British Bank and Consulate in Istanbul Turkey by AQ affiliate (57), 520

---2003: Car bombing outside mosque in Najaf, Iraq by AQ Iraq (125), 520

---2004: Two suicide bombings of political party offices in Irbil, Iraq by Kurdish Terrorists (109), 520

---2004: In N Uganda LRA rebels attacked a refugee camp (192), 520

---2004: Superferry 14 bombing near Manila, Philippines by Abu Sayyaf (116), 520

---2004: Train Bombings in Madrid, Spain (3/11) by Al-Qaeda inspired (191), 521

---2004: Khobar massacre, khobar, Saudi Arabia by AQ affiliate (22), 523

---2004: Multiple suicide bombings at shrines in Kadhimiyah and Karbala, Iraq by Sunni insurgents / AQ in Iraq (188), 523

---2004: Multiple bombings and armed attacks in several cities in Iraq by Sunni Insurgents /AQ in Iraq (103), 523

---2004: School Hostage Crisis, Beslan Russia by Chechen Terrorists (334), 523

---2004: Akhmad Kadyrov (President of Chechnya) assassinated by Chechen Terrorists, 523

---2005: Rafik Hariri (Lebanese Prime Minister) assassinated by Hezbollah, 523

---2005: Amman bombing in Amman, Jordan by AQ affiliate (60), 523

---2005: New Dehli Bombings, India by Pakistan Kashmiri Separatists (62), 523

---2005: Car bombing outside medical clinic in Hilla,Iraq by AQ in Iraq (125), 523

---2005: London Trains & Bus Bombings, UK (7/7) by Al-Qaeda Inspired (52), 524

---2005: Sharm el-Sheikh Resort Attacks, Egypt by Al-Qaeda affiliate (88), 525

---2005: Multiple suicide bombings and shooting attacks in Baghdad, Iraq by AQ in Iraq (182), 525

---2006: Central Mindanao bombings in Philippines by the Moro Islamic Liberation Front (MILF) (8), 525

---2006: Bombings in Karbala, Ramadi, and Baghdad, Iraq by sectarian militants by AQ in Iraq (124), 525

---2006: Multiple bombings on commuter trains in Mumbai, India By Lashkar-e-Tayyiba & Students Islamic Movement of India (SIMI)(200), 525

---2006: Truck bombing of military convoy near Habarana, Sri Lanka by Tamil Tigers (103), 525

---2006: Sadr City bombings in Baghdad, Iraq, by Sunni Insurgents / AQ in Iraq (215), 525

---2007: Multiple bombings in Baghdad area, Iraq by Sunni Insurgents / AQ in Iraq (101), 526

---2007: Truck bombing in market place in Baghdad, Iraq by Sunni Insurgents / AQ in Iraq (137), 526

---2007: Two bombings and other attacks on pilgrims, Hilla, Iraq by Sunni Insurgents / AQ in Iraq (115), 526

---2007: Two truck bombings in Tal Afar, Iraq by Sunni Insurgents / AQ in Iraq (152), 526

---2007: Bombings in Baghdad, Iraq by Sunni Insurgents / AQ in Iraq (193), 526

---2007: Hostage taking by Sunni radicals and subsequent storming of mosque in Islamabad, Pakistan (102), 526

---2007: Multiple truck bombings in Al-Qataniyah and Al-Adnaniyah, Iraq by Sunni Insurgents / AQ in Iraq (796), 526

---2007: Truck bombing in Armi, Iraq by Sunni Insurgents / AQ in Iraq (105), 526

---2007: Bombing of motorcade in Karachi, Pakistan in an attempted assassination of Benazir Bhutto by Pakistan Taliban (137), 526

---2007: Assassination of Benazir Bhutto in Pakistan and others by Pakistan Taliban (24), 527

---2007: Algiers, Algeria bombings by AQ affiliate (33), 527

---2007: Algiers, Algeria bombings by AQ affiliate (60), 527

---2008: Bombing at dog fighting festival in Kandahar, Afghanistan by the Taliban (105), 527

---2008: Mumbai Attacks, India by Lashkar-e-Taiba (164), 527

---2008: American Embassy attack in Sana'a Yemen by Islamic Jihad of Yemen (al-Qaeda affiliate) (19), 527

---2008: Christmas Attacks in N DRC and S Sudan by Lords Resistance Army (865), 527

---2009: Uprising In Borno State Nigeria by Boko Haram (780), 527

---2009: Multiple bombings at government sites in Baghdad, by Sunni Insurgents and AQ in Iraq (102), 527

---2009: Two car bombs explode at government buildings in Baghdad, Iraq carried out by Sunni Insurgents and AQ in Iraq (155), 528

--2009: Bombing at marketplace in Pakistan by Pakistan Taliban militants (118), 528
---2009: Five car bombings in Baghdad, Iraq by Sunni Insurgents/AQ in Iraq (127), 528
---2010: Multiple bombings in Hilla, Basra, al-Suwayra, and other cities, Iraq by Sunni Insurgents and AQ in Iraq (102), 528
---2010: Metro bombings in Moscow Russia by Chechen Terrorists (40), 528
---2010: Attack in Dantewada India by Maoist Terrorists (76), 528
---2010: Bombings in Zahedan, Iran by Jundullah (27), 528
---2010: Kampala, Uganda attacks groups watching Football by Al-Shabab (75), 528
---2010: Bombings in Abuja, Nigeria by MEND (12), 528
---2011: Oslo Bombing/Shootings, Norway by Far Right Extremist (77), 529
---2011: Attacks in Nigeria by Boko Haram (105), 529
---2011: Attacks in Mogadishu against the transitional govt by Al Shabaab (45), 529
---2011: Attack in Jonglei province, South Sudan, by SPLA off shoot (111), 529
---2012: Multiple bombings in Kano, Nigeria by Boko Haram (178), 529
---2012: Bombing in Sana'a, Yemen by Ansar al-Sharia (Al-Qaeda AP affiliated) (120), 529
---2012: Southern Yemen suicide bombing by AQ AP (45), 529
---2013: Syrian Government accused of rocket attacks in Aleppo, Syria (82), 529
---2013: Attacks on Algerian Gas facility by Al-Qaeda in the Islamic Maghreb (AQIM) (40), 529
---2013: Suspected Boko Haram shootings over 3 days (31), 529
---2013: Lashkar-e-Jhangvi bombings in Quetta and elsewhere in Pakistan (126), 529
---2013: Attack on Christian Church in Peshawar, Pakistan by Pakistani Taliban - Jundullah (81), 530
---2013: Kenyan Shopping Centre attack by Al-Shabab (67), 530
---2013: Nigerian College attack by Boko Haram (50), 530
---2013: Attacks in Russia by Chechen Terrorists (20), 530

- Chronology .of the World's Worst Airline attacks by Terrorists, 531-537

---1933: Imperial Airways flight by passenger (15), 532
---1933: United Airlines Boeing 247 by Chicago gang (7), 532
---1949: Canadian Pacific Air Lines DC-3 by a Jeweller (23), 532
---1955: United Airlines Flight 629 (44), 532
---1959: National Airlines Flight 967 (42), 532
---1962: Continental Airlines Flight 11, 532
---1966: Aden Airways DC3 (30), 532
---1967: Cyprus Airways Flight 284 (66), 532
---1970: Swissair Flight 330 (47), 532
---1973: Aeroflot Tu-104 (100), 532
---1976: Cubana Airlines (73), 533
---1976: Middle East Airlines Flight 438 (81), 533
---1976: Air France 139 (4), 533
---1977: Malaysian Boeing 737 (100), 533
---1982: Pan Am Flight 830 (1), 533
---1983: A Gulf Air Boeing 737 (112), 533
---1985: Air India Flight 182 (331), 533
---1986: TWA Flight 840 (4), 533
---1987: Korean Air Flight 858 (115), 533
---1988 - Pan Am Flight 103 (259), 534
---1989: French UTA Flight 772 (171), 535
---1989: A Colombian Avianca Flight 203 (110), 535
---1990: Chinese Boeing 737 (132), 535
---1993: Transair Georgian Airlines Tu-154B (106), 535
---1994: Philippine Airlines Flight 434 / Operation Bojinka (1), 535
---1996: An Ethiopian Boeing 767 (127), 535
---1997: Malaysian Boeing 737 Flight 653 (100), 535
---1999: An Egypt Air Boeing 767 (217), 535
---2001: Attack on America 9/11 (2,997), 536

--2001: American Airlines Flight 63 (0) - the Shoe Bomber, 536
---2002: China Northern Flight 6136 (112), 536
---2004 : Volga-Avia Express Flight 1303 (89), 536
---2006: 10 Airliner Atlantic Plot (0), 536
---2009: Northwest Airlines Flight 253 (0) - Christmas Day bombing / Underpants Bomber, 536
---2010 - UPS Flight 232 & FedEx Cargo Planes, 537

Section 7 - Criminals/Cases

- Introduction, 542
-Corruption

--Individuals/Politically Exposed Persons, 543-560
---Ferdinand Marcos, 543
---Papa Doc & Baby Doc Duvalier, 544
---Manuel Noriega, 544
---Raúl Salinas, 545
---Mobutu Sese Seko, 547
---Augusto Pinochet, 547
---Sani Abacha, 548
---Pavel Lazarenko, 549
---Slobodan Milosevic, 550
---Alberto Fujimori, 550
---Vladimiro Montesinos, 551
---Mohammed Suharto, 552
---Joseph Estrada, 553
---Paulo Maluf, 553
---Arnoldo Aleman, 554
---Frederick Chiluba, 554
---Saddam Hussein, 555
---Ali Zardari - Bhutto, 556
---Teodoro Obiang & Son, 556
---Diepreye Alamieyesiegha, 557
---Randy "Duke" Cunningham, 557
---Omar Bongo, 558
---Zine El Abidine Ben Ali, 558
---Muammar Gaddafi & Son, 559
---Muhammad Hosni Mubarak, 560
---James Ibori, 560

--Corporates, 561-567
---Lockheed Martin, 561
---Bofors, 561
---Thomson CSF -Thales, 562
---Statoil, 563
---BAE Systems, 564
---Siemens, 565
---Kellog Brown & Root, 566
---Macmillan Publishing, 567
---GlaxoSmithKline, 567

--Environmental Crime, 568
---Seveso, 568
---Bhopal, 568
---Chernobyl, 568

-Fraudsters

--Accounting Fraudsters, 569-580

---Alan Bond, 569

---Robert Maxwell, 569

---Ken Lay & Others, 571

---Bernie Ebbers, 575

---Dennis Kozlowski, 576

---Calisto Tanzi, 576

---Helmut Elsner & Others, 577

---B Ramalinga Raju, 578

---Tsuyoshi Kikukawa and Others, 580

--Advance Fee Fraudsters, 581

---Chief Nwude & Banco Noroeste, 581

---Hassan Ali Khan, 581

--Hedge Fund/Investment Co Fraudsters, 582-585

---Jordan Belfort, 582

---Michael Brown, 582

---Samuel Israel III, 583

---Berni Madoff, 583

---Sammy Goldman & Harry Tanner Jr, 585

--Ponzi - Pyramid Schemes, 586-587

---Charles Ponzi, 586

---Ivar Krueger, 587

---Barry Minkow, 587

--Rogue Traders, 588-605

---Nick Leeson, 588

---Toshehide Iguchi, 590

---Kyriacos Papouis, 592

--- Peter Young, 593

---Yasua Hamanaka, 593

---Joseph Jett, 595

---John Rusnak, 596

---Liu Qibing, 599

---David Lee, 599

---Jerome Kerviel, 601

---Frances Yung, 603

---Kweku Adoboli, 604

--Private Banker Fraudsters, 606-607

---Hans Peter Walder, 606

--Tax Fraudsters - Tax Evaders, 607-610

---Mikhail Khodorkovsky, 607

---Operation Wickenby, 608

---Pasquantino Brothers, 609

--Others, 610-611

---Douglas Jackson, 610

---Pokerstars & Others, 611

--Insider Traders, 611-624

---R Foster Winans, 611

---Ivan Boesky & Others, 612

---George Soros, 613

---Ernest Saunders, 614

---James McDermot Jr, 615

--- Martha Stewart, 615

---Philippe Jabre, 616

---Anthony Elgindy & Others, 616

---Michael Guttenberg & Others, 617

---Takafumi Horie, 617

---Chen Rongsheng, 618

---Chris Littlewood & Others, 618

---Nicos Stephanou & Others, 619

---Stanko Grmovsek, 619

---Mehmit Sepil, 620

---Raj Rajaratnam, 620

---Malcolm Calvert, 622

---Oswyn Indra de Silva, 622

---John Hartman, 622

---Winifred Jian & Others, 623

---Joseph Skowron, 623

---US Congress, 624

---David Einhorn & Others, 624

---SAC Capital, 624

--Kidnappers/Robbers/Extortioners/Forgers, 625-629

---Elmyr de Hory, 625

---Gerd Heidemann, 625

---Glico-Morinaga, 625

---Northern Bank / IRA, 626

---Ingrid Betancourt, 627

---The History Men, 628

---Kiyoshi Takayama, 629

--Market Abusers, 629-642

---Tulip Bubble - 1634, 629

---South Sea Company, 630

---William Duer, 631

---London Stocks Exchange Hoaxers of 1814, 632

---NY State Senator Kimble - 1840s, 632

---Daniel Drew & Others, 632

---Stock Market Crash 1929, 633

---Michael J Meehan, 634

---Albert H Wiggin, 634

---Charles Mitchell, 634

---Richard Witney, 634

---The Huni Brothers, 635

---Michael Milken, 635

---John Kaweske, 637

---The Flaming Ferraris, 637

---California Electricity Crisis, 638

---Shell, 639

---Ken Mahaffey & Others, 639

---Simon Eagle, 640

--Christopher McQuoid, 640
--Dipak Patel & Others, 640
--David Mason, 641
--Christopher Pia, 641

-Traffickers

--Illicit Arms Traffickers, 642-649
---Basil Zaharoff, 642
---Adnan Khoshoggi, 643
---Leonid Minin, 643
---Simon Mann, 644
---Mohamed al-Kassar, 645
---Tomislav Damnjanovic, 646
---Pierre Falcone, 646
---Victor Bout, 647

--Drug Traffickers (Organised Crime), 649-654
---The French Connection, 649
---Pizza Connection, 649
---La Mina/Operation Polar Cap, 650
---Lucy Edwards & Peter Berlin, 652
---Speed Joyeros, 653
---Beacon Hill, 653
---Lespan, 653
---Pedro Allatore, 654

--Traffickers (Goods & Human), 655-657
---Operation Pangea & Others, 655
---Robert Mikelsons, 656
-- Operation Bia & Others, 656

--Terrorist Financiers, 658-663
---International Islamic Relief Org (Philippine & Indonesian Branches) (IIRO), 658
---Holy Land Foundation, 658
---Benevolence International Foundation, 659
---Muwafaq Foundation, 660
---Al-Rashid Trust, 660
---The Rabita Trust, 660
---Al Haramain Islamic Foundation (Bosnian & Serbian Offices), 661
---The Afghan Support Committee/Revival of Islamic Heritage Society, 661
---Global Relief Foundation, Taibah International and Al Furqan, 661
---Interpal & Others, 662
---Carnival French Ice Cream, 662
---al-Aqsa Foundation, 663
---Al-Akhtar Trust, 663
---Sanab Charitable Committee, 663

--WMD Proliferation Financiers/Sanctions, 664-668
---Ummah Tameer-e-Nau, 664
---Abdulrahman Alamoudi, 664
---Abdul Qadeer Khan, 666
---Karl Lee, 668

Section 8 - Enforcement Cases
-Introduction, 671-673
-Chronology of Bank/FI Major Enforcement Cases over the last 25 years, 673-674
- Enforcement Cases, 675-738
---Nugan Hand Bank, 675
---Banco Ambrosiano, 675
---Drexel Burnham Lambert, 676
---BCCI, 676
---Salomon Brothers, 678
---Barings Bank, 679
---Daiwa Securities, 679
---Deutsche Morgan Grenfell, 680
---NatWest Markets, 680
---Sumitoma Corporation, 680
---Broadway National Bank, 681
---Global Analyst Research Settlement, 681
---Mutual Fund Scandal, 684
---GLG Partners, 686
---Citigroup Japan, 686
---Citigroup UK, 686
---AmSouth, 687
---Riggs Bank, 687
---Oppenheimer & Company, 690
---UBS, 690
---ABN Amro Bank, 691/709
---City National Bank, 691
---Banco de Chile, New York & Miami Branches, 691
---Pacific National Bank (Banco del Pacifico), 692
---New York Stock Exchange, 692
---Arab Bank, 692
---Banco Delta Asia, 693
---Bank of New York, 694
---Beach Bank, Miami, 695
---The Foster Bank, Chicago, 696
---Israel Discount Bank of New York, 696
---Liberty Bank of New York, 696
---BankAtlantic, 697
---American Express Bank International, 697
---Union Bank of California, 698
---Bank of America, 699
---International Bank of Miami, 700
---Israel Discount Bank, 700
---Mizrahi Tefahot Bank, 700
---E*Trade, 701
---United Bank for Africa, 701
---Sigue Corporation, 702
---The Bank of Tokyo-Mitsubishi UFJ, 702
---Winterflood, 703
---Société Générale, 703
---Aon Limited, 703
---Doha Bank, 703
---E*Trade, 704
---Credit Suisse, 704
---Lloyds Banking Group, 705
---Stanford Bank, 706

--UBS, 708
---ANZ, 708
---Amaranth Advisors LLC, 709
---Royal Bank of Scotland (former ABN Amro Bank), 709/691
---Wachovia Bank, 711
---Barclays Bank, 712
---Deutsche Bank, 713
---Pamrapo Savings Bank, 713
---Goldman Sachs & GS International, 714
---Trillium Capital, 714
---Royal Bank of Scotland, 715
---Merrill Lynch, 715
---Ocean Bank, 715
---Pacific National Bank, 716
---Zions First National Bank, 716
---Mizrahi Tefahot Bank, 716
---JP Morgan Chase Bank, 717
---Deutsche Securities Korea, 717
---Lebanese Commercial Bank, 717
---Turkish Bank (UK), 718
---Mizrahi-Tefahot Bank, 718
---Coutts & Company, 718
---Habib Bank, 719
---HSBC, 719
---UBS, 722
---Wegelin & Co, 722
---ING Bank, 723
---Standard Chartered, 724
---First Bank of Delaware, 724
---Allianz, 724
---Libor Bid Rigging Scandal, 725
---Barclays Bank, 725
----UBS, 726
----Royal Bank of Scotland, 726
----ICAP, 726
----Rabobank, 727
----European Commission Action, 727
---National Bank Abu Dhabi, 728
---MoneyGram, 728
---SAC Capital, 729
---EFG Private Bank, 730
---UBS France, 730
---HSBC Argentina, 731
---HSBC Mexico SA, 731
---Bank of Tokyo Mitsubishi-UFJ Ltd (BTMU), 731
---Barclays, 731
---Nordea AB, 732
---Panther Energy Trading, 732
---Oppenheimer & Co Inc, 733
---American Express, 733
---Guaranty Trust Bank, 733
---JP Morgan Chase, 734
---JP Morgan Chase, 735
---Saddle River Valley Bank, 735
---TCF National Bank, 736

--TD Bank, 735
---Indian Banks, 736
---Swiss Bank Fines, 736
---Royal Bank of Scotland, 736
---Outlook Cases/2014 and beyond, 738

Breaking News

--Part 1, Section 1 - Predicate Crimes
---Bribery & Corruption, 739
---Fraud including Tax Fraud & Cybercrime, 739

---Part 1, Section 2, Sub-section 4 - Country Risks

---Part 1, Section 4 - Laws & Regulations
----AML Treaties, Conventions & Major Laws
----Financial Action Task Force - FATF work in 2014
----The Wolfsberg Group
----Sanctions & Embargoes

---Part 2, Section 5 - Regions, Countries, Criminals & Terrorists

---Part 2, Section 6 - Terrorist Attacks
----2014: Terrorist Attack at Train Station in Kunming, China by Xinjiang extremists (29)
----Numerous attacks by Boko Haram in Nigeria (700)

---Part 2, Section 8 - Enforcement Cases
----JP Morgan Chase
----Standard Bank
----Canada Inc formerly Swift Trade Inc
----Credit Suisse
----Gold Fixing Investigation
----Brown Brothers Harriman
----Forex Probe

Reviews of this Book

"For anyone wanting to delve into the background of financial crime and money laundering, this book is a fine starting point. John Cusack has assembled an amazing amount of information, from types of crime to particular threats faced by individual countries. I would have been a much better informed President of FATF if John's book had been available a few years ago."

Lord James Sassoon, former Commercial Secretary to the Treasury (UK) (2010-2013) and President of the Financial Action Task Force (2007/2008)

"Impressive. A multifaceted reference book containing a wealth of information on a challenging subject."

Boudewijn Verhelst, Head Belgian FIU and Former Chair until 2013 of the Egmont Group of Financial Intelligence Units

"An impressive book indeed, by size and by content from a man who knows what he is talking about and who has been dedicated to the fight against money laundering for at least two decades."

Alexander Karrer, Deputy State Secretary, State Secretariat for International finance, Swiss Federal Department of Finance

"John Cusack's "Red Alert" deserves to become the global standard textbook on AML and CFT for banking practitioners, compliance officers as well as regulators and academics. This is the first publication on the subject written by a true professional and experienced senior AML responsible. John's "Red Alert" accumulates the collective knowledge of some the best compliance officers of our generation. Reflecting 18 years of professional insight and responsibility the book can give profound and practical guidance to experts and shared experience to new joiners. The collection of facts and cases is unique. Everybody should read the introductory five recommendations to "Effectively" combat Money Laundering which sounds like John's message that if we want to win the fight against financial crime all of us have to think about and decide on fundamental changes to the current approach which has come to its limits and, at least partially, failed to achieve what it was originally intended for. Time has come for unbiased reviews and to develop a far more integrated approach. This core message alone and the considerations and facts that lead to it make this book compulsory reading for all those who count in the industry. A great achievement. Congratulations."

Hans-Peter Bauer, Board Member of the Basel Institute, founder member and first Chairman of the Wolfsberg Group and currently senior adviser to the Group.

"Anti-money laundering efforts, both in the prosecution of those engaged in the illicit activities, as well as financial institutions, who are at the forefront of the fight to keep illicit funds from flowing through the financial sector, has become increasingly complex. Attempting to understand all of the potential risks, as well as possible avenues to prevent money laundering and related financial crimes, also has become quite difficult. John's book Red Alert, is an excellent and comprehensive compilation of existing risks and potential solutions, with detailed narratives on how to effectively implement. In addition, John has included a significant number of summaries of actual cases, which provide an excellent framework for anyone truly interested in understanding the root cause of some significant money laundering matters. Understanding the how money laundering occurred, provides for the ability to identify and implement meaningful solutions. While others may have been able to research and bring together some of this information, no one is more uniquely qualified than John to bring together all relevant information in one publication. This a book that will serve as a primary reference for most all things money laundering and financial crime related."

Rick Small, Vice President, enterprise-wide AML and Sanctions Risk Management, American Express. Formerly served as global AML leader for GE Money, Managing Director of Global Anti-Money Laundering at Citigroup and prior to that, as special counsel at the Federal Reserve System with responsibility for all Bank Secrecy Act and money laundering matters. Rick is also a former Co-Chair of the Wolfsberg Group.

"John Cusack is one of the "elders" of the Anti-Money Laundering compliance community. He witnessed the emergence of the discipline more than 20 years ago and he has occupied a leading role in the evolution of the practice of AML compliance ever since. I just wish he looked his age like the rest of us. In Red Alert, John has done the anti-money laundering compliance community and anyone interested in the global fight against financial and organised crime a great service. His book is a valuable resource for practitioners and anyone interested in learning about the origins, challenges and current practice of global AML compliance. Red Alert also provides thoughtful and provocative ideas and concrete proposals to advance the goal of global anti-money laundering law: the interdiction of the vast market in criminal proceeds derived from organised crime, corruption and a wide range of financial crimes. As anyone working in the field of anti-money laundering compliance knows the pace and scale of regulatory AML enforcement against financial institutions has reached historic levels and has been sustained for longer than ever before. AML and financial crime have become significant operational risks for financial institutions throughout the world. John has provided a resource that I predict will find a comfortable place on the bookshelves or e-book devices of compliance officers all over the world."

Kevin J Ford, Managing Director BrightLine GRC LLC New York. Formerly Deputy Commissioner of Investigation for the City of New York and Special Assistant US Attorney for the Southern District of New York, Associate General Counsel in the Business Intelligence Group and Goldman Sachs' first UK Money Laundering Reporting Officer, former Managing Director and Chief Compliance Officer for Regulatory DataCorp (RDC). Mr. Ford is also a member of the Board of Transparency International USA and a member of Interpol's Group of Experts on Corruption.

"The private sector and its Banks play an important role in and contribute to fighting financial crime in many ways. With ever increasing demands and expectations placed upon Banks, John Cusack's excellent Book is a timely and essential resource for financial crime professionals that both demonstrates his own contribution and reflects the nature and extent of contribution from the industry to date."

Sally Scutt, Deputy Chief Executive, British Bankers' Association and Managing Director, International Banking Federation (IBFD)

"For many years now the fight against financial crime and the detection of the proceeds of such activities has been one of the major challenges facing the financial markets. Increasingly financial institutions, financial centres, regulators and governments themselves are at risk of severe reputational damage if they fail to detect such activity. Individuals are also at risk of public censure or worse if they fail to instigate systems and controls to combat the risk of money laundering the proceeds of crime and to prevent their organisation being used by criminals and terrorists. Against this background John Cusack's book is very timely. I do not think anybody is better qualified to address this topic, he has been at the forefront of the fight against financial crime for most of his career and his wisdom and practical approach is very evident throughout. I commend this book to those working in the financial services industry, to the lawyers and compliance personnel who work with them and of course to their regulators, law enforcement agencies and policy makers."

Neil Stocks, former Global Head of Compliance UBS

"John Cusack has been at the leading edge of the banking industry's anti-money laundering agenda for well over a decade. He has compiled here a comprehensive picture of the legislative and regulatory history and international standards that have brought us to where we are today, along with subject matter analysis of cases, typologies, enforcements, and perpetrators. In all this is the 'must have' compendium for anyone constructing or assessing their AML programme, and is a fitting and worthy tribute to Matt Cooper's work."

Alan Williams, Global Head of Financial Crime, Royal Bank of Scotland

"John Cusack offers the reader an insight into a world which is unfortunately only too real, though one many rarely see, in any event with up front clarity and precision drawing from his many years of experience. UBS is only one of many stakeholders who can help in the fight to combat money laundering, a fight that John rightly identified requires still much greater focus on effectiveness and more resourceful co-operation between public and private parties. This at a time when co-operation and trust evidently requires renewed investment. We need to always remember that TRUST IS THE SUM OF ALL PROMISES. Accordingly John lays bare the harms and very significant threats we all face in not working together and in allowing trust to wither. I thank all readers to take this to heart."

Markus Diethelm, UBS Global General Counsel

"This weighty tome amply demonstrates why financial crime deserves a higher priority in both thought and resources, as Mr. Cusack exhorts. All those involved in the challenge should either read this book, or know it already - which given its encyclopaedic quality, is somewhat unlikely."

John Mair, Head of Project Integrity, EBRD; former Group Financial Crime Director, Lloyds Banking Group.

"Perhaps best described as the 'The ultimate guide to Money Laundering detection and prevention'... even experienced Anti-Financial Crime professionals will gain some unique insights from this book on aspects they may have not dealt with (so frequently). The author and contributors are the top of the top in their field and this is a must have reference guide, if you are serious about combating financial crimes. You want to spice up your next presentation with some juicy insights... look no further!"

Markus Schulz, Chief Compliance Officer GE Capital International and former Group Financial Crime Officer Zurich Insurance

"One of the most striking things that comes through on reading John Cusack's excellent book is how often in the financial services industry in particular firms repeat the same mistakes. The similarities between our own recent "rogue trader" and Jerome Kerviel's exploits at Soc Gen is but one striking example. Our greatest weapon to combat such failure is the education of the professionals in the industry and John's book is a major contribution in this regard. It is an invaluable tool for all in the industry, regulator or regulated."

Andrew Williams, General Counsel UBS Wealth Management Retail & Corporates and former UBS Global Head of Compliance

"A compendium, a digest , a manifesto: 'Red Alert ' represents an essential tool for anyone interested in Financial Crime. Whether you are an AML professional, an academic, a regulator, a consultant or just interested in knowing more about how money laundering works , how financial institutions are impacted by it and the ways they try to prevent and detect it, you will find this book invaluable. Written by one of the financial industry's most respected practitioners, it represents an excellent resource as well as advocating practical ways in which the fight against financial crime could be made more effective."

Chris Davies, APAC General Counsel, SocGen, former SocGen Group Compliance Head and Wolfsberg Group Co-Chair (2010-2013)

"John Cusack's reputation as a leading thinker and practitioner in the bank compliance field is well-established and will be re-inforced by this path breaking volume. Perhaps less appreciated is John's more longstanding membership in a less saintly trade. The broad thematic treatment and trenchant case study analysis displayed here derive in large part from his legal background. The one-two punch this book delivers sets John apart, and commends this work to compliance and legal professionals. Indeed one submits that lawyers may have the most to learn from perusing it."

Marc Cohen, Partner, Regulatory & Financial Crime, Mayer Brown

"All you ever needed to know about financial crime"

Heidi Suila, Head of Financial Crime Compliance, Nordea

"Everything you always wanted to know about money laundering but were too afraid to ask". John Cusack's book is not only an impressive and exhaustive compilation of facts and figures about the global fight against money laundering: it is the key to understand what is really at stake in this fight. A must read for anyone really interested in understanding and combating money laundering."

Stephane Tourette, Head Legal Wealth Management, Banque Pictet & Cie

"John Cusack's magnificent treatise on money laundering and financial crime reminds those of us who are daily following our respective firms' anti-money laundering procedures why we are doing this. With only a 1% detection rate, the war on financial crime, drug dealing and terrorism has a long way to go. Just one example from the many John identifies: although the former President Marcos of the Philippines is believed to have stolen \$5 billion to \$10 billion from the country,

and yet some 28 years later, less than \$700 million has been recovered. To prevent crime, criminals need to know that crime does not pay. Money, and the flow of money through banks and other institutions and corporates, is the life blood of crime. Hence the need for strong and effective global anti-money laundering programmes.

John's book will undoubtedly become the "go to" reference work for anyone involved in anti-money laundering procedures and the wider fraud community of professionals . This is deservedly so, as it is well researched, well evidenced and of enormous breadth and depth. John is to be congratulated for his determination and stamina in completing such a work."

Noel Campbell, Partner, Head of the Fraud & Insolvency Group, Holman Fenwick Willan LLP

