ACAMS

Certified Anti-Money Laundering Specialist

STUDY GUIDE

Version 6.46

acams.org

Credits and Copyright

CAMS Examination Task Force

Task Force Executive Chair
John J. Byrne, CAMS
Project Manager
Catalina Martinez

We would like to thank the following individuals for their significant contribution in the development of the CAMS Examination and Study Guide through the work of the CAMS Examination Task Force.

Bob Pasley, CAMS– *Task Force Chair*
Kevin Anderson, CAMS– *Task Force Chair*
Brian Stoeckert, CAMS– *Task Force Chair*
Paul Osborne, CAMS– *Task Force Chair*
Peter Wild, CAMS-Audit– *Task Force Vice Chair*
Barbara Keller, CAMS– *Task Force Vice Chair*
Hue Dang, CAMS-Audit *(ACAMS Asia)*
Samantha Sheen, CAMS *(ACAMS Europe)*
David Clark, CAMS–*ACAMS Advisory Board*
Anna Rentschler, CAMS–*ACAMS Advisory Board*
Rick Small, CAMS–*ACAMS Advisory Board*
Nancy Saur, CAMS–*ACAMS Advisory Board*
Vasilios Chrisos, CAMS–*ACAMS Advisory Board*
Dennis Lormel, CAMS–*ACAMS Advisory Board*

Abbas Bou Diab, CAMS
Angel Nguyen, CAMS
Brian Vitale, CAMS-Audit
Brigette K. Miller, CAMS
Christopher Bagnall, CAMS
Christopher Randle, CAMS-Audit, CAMS-FCI
Dave Dekkers, CAMS-Audit
Deborah Hitzeroth, CAMS-FCI
Kenneth Simmons, CAMS-Audit
Kok Cheong Leong, CAMS-Audit
Lauren Kohr, CAMS-Audit
Lindsay Dastrup, CAMS-Audit
Margaret Silvers, CAMS
Martin Dilly, CAMS-Audit
Nancy Lake, CAMS-Audit, CAMS-FCI
Peter Warrack, CAMS

Donna Davidek, CAMS-Audit
Ed Beemer, CAMS-FCI
Eric Wathen, CAMS
Gary Bagliebter, CAMS
Iris Smith, CAMS-Audit
Iwona Skornicka Castro, CAMS
Jack Sonnenschein, CAMS-Audit
Jeremy Brierley, CAMS
Jim Vilker, CAMS
Joel Conaty

Jurgen Egberink, CAMS
Ana Padilla, CAMS
André Castro Carvalho, CAMS
Jun Zhu, CAMS
Judith Assouly, CAMS
Holger Pauco-Dirscherl, CAMS-RM, CAMS-Audit, CGSS

Rachele Byrne, CAMS
Sean McCrossan, CAMS-FCI
Sharon McCullough, CAMS
Steve Gurdak, CAMS
Susan Cannon, CAMS-Audit
Susanne Wai Yin Ong, CAMS
Tatiana Turculet, CAMS
Venus Edano, CAMS
William Aubrey Chapman, CAMS-Audit
Yevgeniya Balyasna-Hooghiemstra, CAMS
Zachary Miller, CAMS-FCI
Ahmad Tarteer, CAMS-Audit, CGSS
Joyce Hsu, CAMS-FCI
Jung Hyun Choi, CAMS
Terumasa Kaku, CAMS
Gina Storelli, CAMS-Audit

ACAMS would also like to thank the ACAMS Chapters worldwide for their contribution in the development of the CAMS Examination.

ACAMS

ACAMS Product Staff

Eric Solecki	Ronald Myers	Edith Velasquez
Astrid Rouleau, CAMS	Brenda Fewox	Tiffany Alcorn
Amanda J. Dominique	Marco Tham, CAMS	Charles Ball
Michelle Rance, CAMS	Heather Carroll	Shannon Field
Yuen Cho Man, CAMS	Crystal Ferguson	Adam Cochran
Lindsay Pfisterer	Leslie Smith	Iliana Colón, CAMS
Nancy Peterson	Meghan Cleereman Shull	Todd Beck, CAMS
Melinda Fleming		

This document is designed to be printed in black and white.

ISBN:978-0-9777495-2-2

Table of Contents

Introduction

About ACAMS

The mission of ACAMS is to advance the professional knowledge, skills and experience of those dedicated to the detection and prevention of money laundering around the world, and to promote the development and implementation of sound anti-money laundering policies and procedures. ACAMS achieves its mission through

- promoting international standards for the detection and prevention of money laundering and terrorist financing;
- educating professionals in private and government organizations about these standards and the strategies and practices required to meet them;
- certifying the achievements of its members; and
- providing networking platforms through which AML/CFT professionals can collaborate with their peers throughout the world.

ACAMS sets professional standards for anti-financial crime practitioners worldwide and offers them career development and networking opportunities. In particular, ACAMS seeks to

- help AML professionals with career enhancement through cutting-edge education, certification and training. ACAMS acts as a forum where professionals can exchange strategies and ideas;
- assist practitioners in developing, implementing and upholding proven, sound AML practices and procedures; and
- help financial and non-financial institutions identify and locate individuals with the Certified Anti-Money Laundering (CAMS) designation in the rapidly expanding AML field.

About the CAMS Designation

As money laundering and terrorist financing threaten financial and nonfinancial institutions and societies as a whole, the challenge and the need to develop experts in preventing and detecting financial crime intensifies. ACAMS is the global leader in responding to that need, having helped standardize AML expertise by creating the CAMS designation.

Internationally recognized, the CAMS credential identifies those who earn it as possessing specialized AML knowledge. AML professionals who earn the CAMS designation position themselves to be leaders in the industry and valuable assets to their organizations.

Congratulations on your decision to pursue the most respected and widely recognized international credential in the AML field. We welcome and invite you to embark on a journey that may lead you to career advancement, international recognition and respect among peers and superiors.

Read on, study hard and good luck!

Risks and Methods of Money Laundering and Terrorist Financing

Overview

What Is Money Laundering?

Money laundering involves taking criminal proceeds and disguising their illegal sources in order to use the funds to perform legal or illegal activities. Simply put, money laundering is the process of making dirty money look clean.

When a criminal activity generates substantial profits, the individual or group involved must find a way to use the funds without drawing attention to the underlying activity or persons involved in generating such profits. Criminals achieve this goal by disguising the source of funds, changing the form of the currency, or moving the money to a place where it is less likely to attract attention. Criminal activities that lead to money laundering (i.e., predicate crimes) can include illegal arms sales, narcotics trafficking, contraband smuggling, and other activities related to organized crime, embezzlement, insider trading, bribery, and computer fraud schemes.

Formed in 1989, the Financial Action Task Force (FATF) is an intergovernmental body created by the Group of Seven industrialized nations to set standards and foster international action against money laundering. One of FATF's early accomplishments was to dispel the notion that money laundering only involves cash transactions. Through several money laundering typologies exercises, FATF demonstrated that money laundering can be achieved through virtually every medium, financial organization, and business.

The United Nations 2000 Convention against Transnational Organized Crime, also known as the Palermo Convention, defines money laundering as:

- The conversion or transfer of property, knowing it is derived from a criminal offense, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions
- The concealment or disguise of the true nature, source, location, disposition, movement, or rights with respect to or ownership of property, knowing that it is derived from a criminal offense
- The acquisition, possession, or use of property, knowing at the time of its receipt that it was derived from a criminal offense or from participation in a crime

An important prerequisite in the definition of money laundering is knowledge. In all three of the definitions above is the phrase "knowing that it is derived from a criminal offense," and a broad interpretation of knowing is generally applied. In fact, FATF's 40 Recommendations on Money Laundering and Terrorist Financing and the Sixth European Union Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing state that "The intent and knowledge required to prove the offense of money laundering includes the concept that such a mental state may be inferred from objective factual circumstances."

Several jurisdictions also use the legal principle of willful blindness in money laundering cases to prove knowledge. Courts define willful blindness as the "deliberate avoidance of knowledge of the facts" or "purposeful indifference" and have held that willful blindness is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction.

After the events on September 11, 2001, in October 2001, FATF expanded its mandate to address countering the financing of terrorism (CFT). Both terrorists and money launderers can use the same methods to move their money in ways to avoid detection, such as structuring payments to avoid reporting and use of underground banking or value transfer systems (e.g., hawala, hundi, and fei ch'ien). However, while funds destined for money laundering are derived from criminal activities, such as drug trafficking and fraud, terrorist financing can include funds from perfectly legitimate sources.

Concealment of funds used for terrorism is primarily designed to hide the purpose for which these funds are used, rather than their source. Terrorist funds might be used for operating expenses, including paying for food, transportation, and rent, as well as for the actual material support of terrorist acts. Terrorists, similar to criminal enterprises, value the secrecy of transactions regarding their destination and purpose.

In February 2012 (and amended periodically since), FATF published a revised list of its 40 recommendations, which includes a new recommendation addressing ways to prevent, suppress, and disrupt the proliferation of weapons of mass destruction (WMD).

Three Stages of the Money Laundering Cycle

Money laundering often involves a complex series of transactions that are difficult to separate. However, it is common to think of money laundering as occurring in three stages.

Stage One: Placement—The physical disposal of cash or other assets derived from criminal activity.

During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos, and other legitimate businesses, both domestic and international.

Examples of placement transactions include the following:

- Blending of funds: Commingling illegitimate funds with legitimate funds, such as placing the cash from illegal narcotics sales into a cash-intensive locally owned restaurant
- Purchasing significant stored value cards with currency
- Foreign exchange: Purchasing foreign exchange with illegal funds
- Breaking up amounts: Dividing cash into small amounts and depositing it into numerous bank accounts in an attempt to evade reporting requirements

- Currency smuggling: Cross-border, physical movement of cash or monetary instruments
- Loans: Repayment of legitimate loans using laundered cash

Stage Two: Layering—The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds.

The second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obscure the source and ownership of funds.

Examples of layering transactions include:

- Electronically moving funds from one country to another and dividing them into advanced financial options and/or markets
- Moving funds from one financial institution to another or within accounts at the same institution
- Converting the cash placed into monetary instruments
- Reselling high-value goods and prepaid access or stored value products
- Investing in real estate and other legitimate businesses
- Placing money in stocks, bonds, or life insurance products
- Using shell companies to obscure the ultimate beneficial owner and assets

Stage Three: Integration—Supplying apparent legitimacy to illicit wealth through the reentry of the funds into the economy in what appears to be normal business or personal transactions.

The third stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for example, might choose to invest the funds in real estate, financial ventures, or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal funds. This stage gives a launderer the opportunity to increase his wealth with the proceeds of crime. Integration is generally difficult to identify unless there are great disparities between a person's or company's legitimate employment, business, or investment ventures and a person's wealth or a company's income or assets.

Examples of integration transactions include:

- Purchasing luxury assets, such as property, artwork, jewelry, and high-end automobiles
- Entering into financial arrangements and other ventures in which investments can be made in business enterprises

The Economic and Social Consequences of Money Laundering

Money laundering is a result of any crime that generates profits for the criminals involved. It knows no boundaries, and jurisdictions in which there are weak, ineffective, or inadequate anti-money laundering (AML) and CFT legislation and regulations are most vulnerable. However, large, well-developed financial centers are also vulnerable to laundering due to the large volumes of transactions that allow the launderer to blend in, as well as the wide range of services that enable the launderer to conduct transactions in a way that is convenient. Because most launderers want to eventually use the proceeds of their crimes, their ultimate intent is to move funds through stable financial systems.

Money laundering has significant negative economic and social consequences, especially for developing countries and emerging markets. The easy passage of funds from one organization to another, or relatively facile systems that allow money to be placed without raising any questions, is fertile territory for money launderers. The upholding of legal, professional, and ethical standards is critical to the integrity of financial markets.

The potential macroeconomic consequences of unchecked money laundering include:

- Increased exposure to organized crime and corruption
- Undermining the legitimate private sector
- Weakening financial organizations
- Dampening effect on foreign investments
- Loss of control of, or mistakes in, decisions regarding economic policy
- Economic distortion and instability

- Loss of tax revenue
- Risks to privatization efforts
- Reputation risk for the country
- Risk of international sanctions
- Social costs
- Reputational risk
- Operational risk
- Legal risk
- Concentration risk

Increased Exposure to Organized Crime and Corruption

Successful money laundering enhances the profitable aspects of criminal activity. When a country is seen as a haven for money laundering, it can attract people who commit crimes.

Typically, havens for money laundering and terrorist financing have:

- Limited numbers of predicate crimes for money laundering (i.e., criminal offenses that would permit a jurisdiction to bring a money laundering charge)
- Limited types of organizations and persons covered by money laundering laws and regulations
- Little to no enforcement of the laws and weak penalties or provisions that make it difficult to confiscate and freeze assets related to money laundering
- Limited regulatory capacity to effectively monitor and supervise compliance with money laundering and terrorist financing laws and regulations

If money laundering is prevalent, there is more likely to be corruption. Typically, the penetration of organized crime groups in a jurisdiction is directly linked to public and private sector corruption. Criminals might try to bribe government officials, lawyers, and employees of financial and nonfinancial organizations so they can continue to run their criminal businesses.

In countries with weaker laws and enforcement, it is often corruption that triggers money laundering. It also leads to increases in the use of bribery in financial organizations, among lawyers and accountants, in the legislature, in enforcement agencies, with police and supervisory authorities, and even with courts and prosecutors.

A comprehensive AML/CFT framework, on the other hand, helps curb criminal activities, eliminates profits from such activities, and discourages criminals from operating in a country, especially where law is fully enforced and the proceeds from crime are confiscated.

Undermining the Legitimate Private Sector

One of the most serious microeconomic effects of money laundering is felt in the private sector.

Money launderers are known to use front companies, that is, businesses that appear legitimate and engage in legitimate business, but are in fact controlled by criminals who commingle the proceeds of illicit activity with legitimate funds to hide the unlawful gains. These front companies have a competitive advantage over legitimate firms because they have access to substantial illicit funds, allowing them to subsidize products and services sold at below-market rates. This makes it difficult for legitimate businesses to compete against front companies. Clearly, the management principles of these criminal enterprises are not consistent with traditional free market principles, which results in further negative macroeconomic effects.

By using front companies, particularly multiple front companies, and other investments in legitimate companies, money laundering proceeds can be used to control whole industries and sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxes, thus depriving the country of revenue.

Weakening Financial Organizations

Money laundering and terrorist financing can harm the soundness of a country's financial sector. They can negatively affect the stability of individual banks and other financial organizations, such as securities firms and insurance companies. Criminal activity has been associated with several bank failures around the globe, including the closures of the first Internet bank, European Union Bank, and Riggs Bank. The establishment and maintenance of an effective AML/CFT program is usually part of a financial organization's charter to operate; noncompliance can result not only in significant civil money penalties but also in the loss of its charter.

Dampening Effect on Foreign Investments

Although developing economies cannot afford to be overly selective about the sources of capital they attract, there is a dampening effect on foreign direct investment when a country's commercial and financial sectors are perceived to be compromised and subject to the influence of organized crime. To maintain a business-friendly environment, these impedances need to be eliminated.

Loss of Control of, or Mistakes in, Decisions Regarding Economic Policy

Due to the significant amounts of money involved in the money laundering process, in some emerging market countries, these illicit proceeds might dwarf government budgets. This can result in the loss of control of economic policy by governments or in policy mistakes due to measurement errors in macroeconomic statistics.

Money laundering can adversely affect currencies and interest rates, as launderers reinvest funds where their schemes are less likely to be detected, rather than where rates of return are higher. Volatility in exchange and interest rates due to unanticipated cross-border transfers of funds can also occur. To the extent that money demand appears to shift from one country to another because of money laundering—resulting in misleading monetary data—it can have adverse consequences for interest and exchange rate volatility. This is particularly true in economies based on the US dollar, as the tracking of monetary aggregates becomes more uncertain. Last, money laundering can increase the threat of monetary instability due to the misallocation of resources from artificial distortions in asset and commodity prices.

Economic Distortion and Instability

Money launderers are not primarily interested in profit generation from their investments, but rather in protecting their proceeds and hiding the illegal origin of the funds. Thus, they invest their money in activities that are not necessarily economically beneficial to the country where the funds are located. Furthermore, when money laundering and financial crime redirect funds from sound investments to low-quality investments that hide their origin, economic growth can suffer.

Loss of Tax Revenue

Of the many underlying forms of illegal activity, tax evasion is perhaps the one with the most obvious macroeconomic impact. Money laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case.

A government revenue deficit is at the center of economic difficulties in many countries, and correcting it is the primary focus of most economic stabilization programs. The International Monetary Fund (IMF) has been involved in efforts to improve the tax collection capabilities of its member countries, and the Organisation for Economic Co-operation and Development (OECD) has been instrumental in moving many jurisdictions toward tax transparency.

Risks to Privatization Efforts

Money laundering threatens the efforts of many states trying to introduce reforms into their economies through the privatization of state-owned properties, such as land, resources, and enterprises. Sometimes linked with corruption or inside deals, a government might award a state privatization tender to a criminal organization potentially at an economic loss to the public. Moreover, while privatization initiatives are often economically beneficial, they can also serve as a vehicle to launder funds. In the past, criminals have been able to purchase ports, resorts, casinos, and other state properties to hide their illicit proceeds and facilitate their criminal activities.

Reputation Risk for the Country

A reputation as a money laundering or terrorist financing haven can harm development and economic growth in a country. It diminishes legitimate global opportunities because foreign financial organizations find that the extra scrutiny involved in working with organizations in money laundering havens is too expensive.

Legitimate businesses located in money laundering havens can also suffer from reduced access to markets (or might have to pay more to have access) due to the extra scrutiny of ownership and control systems. Once a country's financial reputation is damaged, rebuilding it is very difficult. It requires significant resources to rectify a problem that could have been prevented with proper AML controls. Other effects include specific countermeasures that can be taken by international organizations and other countries and reduced eligibility for governmental assistance.

Risk of International Sanctions

In order to protect the financial system from money laundering and terrorist financing, the United States, United Nations, European Union, and other governing bodies may impose sanctions against foreign countries, entities, individuals, terrorists and terrorist groups, drug traffickers, and other security threats. In the United States, the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions.

Countries can be subject to comprehensive or targeted sanctions. Comprehensive sanctions prohibit virtually all transactions with a specific country. Targeted sanctions prohibit transactions with specified industries, entities, or individuals listed on OFAC's Specially Designated Nationals and Blocked Persons (SDN) list. Failure to comply can result in criminal and civil penalties.

FATF also maintains a list of jurisdictions identified as high risk and noncooperative, where AML/CFT regimes have strategic deficiencies and do not meet international standards. As a result, FATF calls on its members to implement countermeasures against these jurisdictions, such as financial organizations applying enhanced due diligence (EDD) to business relationships and transactions with natural and legal persons from an

identified jurisdiction in an attempt to persuade it to improve its AML/CFT regime.

Social Costs

Significant social costs and risks are associated with money laundering. Money laundering is integral to maintaining the profitability of crime. It also enables drug traffickers, smugglers, and other criminals to expand their operations. This drives up the cost of government expenses and budgets to combat the serious consequences that result, due to the need for increased law enforcement and other expenditures (e.g., increased healthcare costs for treating drug addicts).

Financial organizations that rely on the proceeds of crime face great challenges in adequately managing their assets, liabilities, and operations, as well as in attracting legitimate clients. They also risk being excluded from the international financial system. The adverse consequences of money laundering are reputational, operational, legal, and concentration risks, and they include:

- Loss of profitable business
- Liquidity problems through withdrawal of funds
- Termination of correspondent banking facilities
- Investigation costs and fines
- Asset seizures
- Loan losses
- Reduced stock value of financial organizations

Reputational Risk

Adverse publicity regarding an organization's business practices and associations, whether accurate or not, will cause a loss of public confidence in the integrity of the organization. As an example, reputational risk for a bank represents the potential that borrowers, depositors, and investors might stop doing business with the bank because of a money laundering scandal.

The loss of high-quality borrowers reduces profitable loans and increases the risk of the overall loan portfolio. Depositors might withdraw their funds. Moreover, funds placed on deposit with a bank could be unreliable as a source of funding once depositors learn that the bank might not be stable. Depositors could be more willing to incur large penalties rather than leave their funds in a questionable bank, resulting in unanticipated withdrawals and causing potential liquidity problems.

Operational Risk

The potential for loss results from inadequate internal processes, personnel, or systems, or from external events. Such losses can occur when organizations incur reduced or terminated inter-bank or correspondent banking services or an increased cost for these services. Increased borrowing or funding costs are also a component of operational risk.

Legal Risk

There is potential for lawsuits, adverse judgments, unenforceable contracts, fines and penalties that generate losses, increased expenses for an organization, and even the closure of the organization. For example, legitimate customers could become victims of a financial crime, lose money, and sue the financial organization for reimbursement. There could be investigations conducted by regulators and/or law enforcement authorities, resulting in increased costs, as well as fines and other penalties. Also, certain contracts could be unenforceable due to fraud on the part of the criminal customer.

Concentration Risk

The potential for loss results from too much credit or loan exposure to one borrower or group of borrowers. Regulations usually restrict a financial

organization's exposure to a single borrower or group of related borrowers. Lack of knowledge about a specific customer, who controls the customer, or the customer's relationships to other borrowers can place an organization at risk in this regard. This is particularly a concern when there are related counterparties, connected borrowers, and a common source of income or assets for repayment. Loan losses can also result from unenforceable contracts and contracts made with fictitious persons.

For these reasons, international bodies have issued statements, such as the Basel Committee on Banking Supervision's guidelines on the *Sound Management of Risks Related to Money Laundering and Financing of Terrorism* and *FATF's International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.*

Economic and social consequences of money laundering (Case example)

In 2017, in Minneapolis, Minnesota, US, 21 people were indicted on sex trafficking and money laundering charges. The organized crime group (OCG) allegedly trafficked women from Thailand to cities across the US for sexual exploitation.

The OCG dealt primarily in cash and conducted a sophisticated international money laundering ring to promote, redistribute, and conceal illegal profits. Funnel accounts were used to launder and route cash from cities across the US to money launderers in Los Angeles. A funnel account is a money laundering method that exploits branch networks of financial institutions. It involves depositing illegal funds into an account at one geographic location and giving criminals immediate access to the money via withdrawals in a different geographic location. The transaction amounts are kept under the AML reporting requirements in an attempt to avoid detection. In this case, funds were withdrawn in Los Angeles and then wired, transported as bulk cash, or mailed to Thailand.

Through the coordinated efforts of various government and enforcement agencies, the human trafficking ring was taken down. The investigation resulted in 20 arrests, recovery of victims from active houses of prostitution, and seizures of hundreds of thousands of dollars in cash and numerous

weapons. The indictment consisted of predicate crimes including sex trafficking, fraud, human trafficking, threats of force, and money laundering.

The victims in this case were primarily poor women with limited ability to speak English. They were promised a better standard of living in exchange for US$40,000 to $60,000 in bondage debt. Criminals gained information about their families and used it to threaten the women and prevent them from fleeing and becoming noncompliant.

The operatives of the money laundering ring helped their victims attain fraudulent visas and travel documents by forging bank statements and creating fictitious backgrounds and employment information. In the US, victims were escorted by a member of the OCG organization to a bank and instructed to open accounts in their own names. OCG members then took control of the accounts and provided the account information to co-conspirators to coordinate deposits throughout the US.

The OCG recruited money mules to carry large volumes of cash on trips to Thailand and used a hawala system to transfer money to Thailand. The OCG moved tens of millions of dollars in illegal proceeds from the US to Thailand and elsewhere using this system.

Collaboration between law enforcement and the private sector is essential to identify money laundering red flags. In addition, organizations must have mechanisms in place to report suspicious activities to regulators and law enforcement in the continuous fight against financial crime. Organizations need to sufficiently train frontline officers to identify fraudulent documents and red flags associated with human trafficking.

Money laundering undermines the legitimacy of the private sector and weakens the financial sector, both of which are critical for a nation's economic growth. Criminals often exploit loopholes within various institutions to facilitate financial crimes. This method undermines the legitimate financial system and exploits various markets, such as the labor market. Money laundering also promotes crime and corruption, which slow economic growth and cause significant reputational risk. In addition, money laundering perpetuates other crimes, such as human trafficking and smuggling, fraud, and corruption. These predicate crimes exploit and victimize vulnerable individuals.

Key takeaways

- Money laundering promotes crime and corruption and slows economic growth.
- Money laundering exploits institutional loopholes and undermines the legitimate financial system and markets.
- Money laundering perpetuates other crimes, such as smuggling, fraud, and corruption.
- Collaboration among various agencies and the private and public sector is necessary to fight financial crime.

AML/CFT Compliance Programs and Individual Accountability

Regulatory guidance and legislation place individual accountability at the senior levels of regulated entities when they have contributed to deficiencies in AML/CFT and sanctions compliance programs.

In 2014, the Financial Crimes Enforcement Network (FinCEN) of the US Department of the Treasury and the US financial intelligence unit (FIU) issued an advisory to financial organizations, reminding them to maintain a strong culture of compliance and specifying that the entire staff is responsible for AML/CFT compliance. This advisory was followed in 2015 by a memorandum on "Individual Accountability for Corporate Wrongdoing" from the US Department of Justice's Deputy Attorney General, Sally Quillian Yates.

The Yates Memo, as it is often referred to, reminds prosecutors that criminal and civil investigations into corporate misconduct should also focus on individuals who perpetrated the wrongdoing. Further, it notes that the resolution of a corporate case does not provide protection to individuals from criminal or civil liability. Although the Yates Memo does not specifically address AML/CFT compliance, enforcement actions issued by US regulators against financial organizations demonstrate a continued focus on AML/CFT compliance deficiencies.

In the United Kingdom, the Financial Conduct Authority (FCA) published final rules for the Senior Managers and Certification Regime (SM&CR), which are

designed to improve individual accountability within the banking sector. In relation to financial crime, the SM&CR requires a financial organization to give explicit responsibility to a senior manager, such as an executive-level money laundering reporting officer (MLRO), for ensuring that its efforts to combat financial crime are effectively designed and implemented. The senior manager is personally accountable for any misconduct within the organization's AML/CFT regime.

The New York State Department of Financial Services (DFS) issued a Final Rule requiring regulated organizations to maintain "transaction monitoring and filtering programs" reasonably designed to monitor transactions after their execution for compliance with the Bank Secrecy Act (BSA) and AML laws and regulations, including suspicious activity reporting requirements, and prevent unlawful transactions with targets of economic sanctions administered by OFAC.

This Final Rule, which went into effect on January 1, 2017, includes very specific requirements concerning the implementation of transaction monitoring systems, including:

- **Risk-Based Models:** Models should be risk-based and commensurate with the organization's own risk assessment and profile.
- **Model Performance Calibration:** Organizations must perform ongoing analysis and testing of the AML/CFT models to assess the scenario logic, performance, model technology, assumptions, and model parameter settings.
- **End-to-End, Pre- and Post-Model Implementation Testing:** End-to-end testing is required to ensure rules are validated and data are complete and accurate.

This Final Rule also requires regulated organizations' boards of directors or senior officers to annually certify to the DFS that they have taken all steps necessary to comply with transaction monitoring and filtering program requirements.

Although the law may seem New York-specific on its face, numerous foreign banks are subject to the law because they operate in New York. Specifically, the law covers banks, trust companies, private bankers, savings banks, and savings and loan associations chartered pursuant to the New York Banking Law, as well as all branches and agencies of foreign banking corporations

licensed pursuant to the Banking Law to conduct banking operations in New York. Moreover, the law also applies to nonbank financial organizations with a banking law license, such as check cashers and money transmitters.

Individual accountability and consequences (Case example)

In August of 2020, the UK's Solicitors Disciplinary Tribunal suspended and fined lawyer Steven David Kinch for repeatedly breaching his professional anti-money laundering obligations.

It is well-known that several legal options exist globally to impose corporate liability. For example, in vicarious liability, an organization could be found criminally liable for the acts of its employees. There is, however, increasing focus on individual liability for professionals when their behaviors and actions encourage, tolerate, or lead to regulatory violations or criminal activity. Individuals are now expected to conduct business responsibly and prevent AML/CFT violations.

Individual professionals are increasingly being held accountable for sector-specific crimes, through prosecution of linked financial crime offenses such as fraud. They may also be held accountable for their organizations' AML/CFT failures. When prosecuted, individuals have been imprisoned, fined, suspended, or debarred from professional activities in regulated sectors.

On August 12, 2020, the UK Solicitors Disciplinary Tribunal suspended lawyer Steven David Kinch for repeatedly breaching his professional anti-money laundering obligations. Kinch failed to check source of funds and perform customer and third-party due diligence when establishing new business relationships. He did not review transactions while doing business with a company incorporated in Sinaloa, Mexico. In fact, he stated that transactions involving foreign nationals and overseas residents, in a location where he had no connection or profile himself, did not raise red flags for him. He admitted that the nature of the transactions being conducted was out of his expertise. Kinch's actions amounted to serious misconduct with high culpability and harm involving significant monies over a three-year period. Kinch was suspended from practice as a lawyer for 15 months and fined £5,000, after which he would be banned from practicing as a sole practitioner, manager, or owner of an authorized or recognized body. He was also forbidden from

acting as a compliance officer for legal practice or finance and administration for three years.

Compliance professionals must recognize the risks and specific accountability that they personally face in their work environments. They should ensure that they are fully up-to-date with legislative and regulatory requirements specific to their role and sector. If they have any concerns regarding integrity or behavior within their firm or business, they should escalate issues through the appropriate formal reporting or whistleblowing channels and document the fact.

Key takeaways

- Regulators use powers to sanction professionals who commit crimes from their sectors.
- Criminal courts can impose a range of sanctions against guilty professionals, including prosecution and imprisonment.
- Accountability for money laundering offenses in a professional capacity can have devastating financial, personal, and reputational consequences for individuals.

Methods of Money Laundering

Money laundering is a constantly evolving activity; it must be continuously monitored in all its various forms for countermeasures to be timely and effective. Illicit money can move through numerous commercial channels, including products such as checking, savings, and brokerage accounts; loans; wires and transfers; and financial intermediaries, such as trusts and company service providers, securities dealers, banks, and money services businesses.

Money launderers operate in and around the financial system in a manner that best fits the execution of the scheme to launder funds. Since many governments around the world have implemented AML/CFT obligations for the banking sector, a shift in laundering activity into the nonbank financial sector and nonfinancial businesses and professions has risen.

FATF and FATF-style regional bodies (FSRBs) publish periodic typology reports to monitor changes and better understand the underlying

mechanisms of money laundering and terrorist financing. The objective of these reports is to provide information on the key methods and trends in these areas and to ensure that the FATF 40 Recommendations remain effective and relevant. This Study Guide refers often to these typologies because they serve as clear examples of how money can be laundered through different methods and in different settings.

Banks and Other Depository Institutions

Electronic Transfer of Funds

Banks have historically been and continue to be important mechanisms in all three stages of money laundering. This section outlines some specific areas of interest and concern for money laundering through banks and other depository institutions.

An electronic transfer of funds is any transfer of funds that is initiated by electronic means, such as internet-based transfers, an automated clearing house (ACH), an automated teller machine (ATM), mobile telephones, and other devices. Electronic funds transfers can happen within a country and across borders. Trillions of dollars are transferred in millions of transactions each day, because it is one of the fastest ways to move money.

Systems such as the US Federal Reserve wire network, or Fedwire, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), and the Clearing House Interbank Payments System (CHIPS) move millions of wires and transfer messages daily. As such, illicit fund transfers can be easily hidden among the millions of legitimate transfers that occur each day. For example, money launderers might initiate unauthorized domestic or international electronic transfers of funds—such as ACH debits or cash advances on a stolen credit card—and place the funds into an account established to receive the transfers. Another example is stealing credit cards and using the funds to purchase merchandise that can be resold to provide the criminal with cash.

Money launderers also use electronic transfers of funds in the layering stage of the laundering process. The goal is to move the funds from one account to another, from one bank to another, and from one jurisdiction to another with each layer of transactions—making it more difficult for law enforcement and investigative agencies to trace the origin of the funds.

To avoid detection at any stage, money launderers can take basic precautions, such as varying the amounts sent, keeping the transfers relatively

small and under reporting thresholds, and, when possible, using reputable organizations.

The processes in place to verify electronic transfers of funds have been tightened. Transaction monitoring software providers have developed sophisticated algorithms to help detect and trigger alerts that might indicate money laundering or other suspicious activity using electronic transfers of funds. However, no system is foolproof.

Following are some indicators of money laundering using electronic transfers of funds:

- Funds transfers occur to or from a financial secrecy haven or high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- Large incoming funds transfers are received on behalf of a foreign client, with little or no explanation or apparent reason.
- Checks and money orders are used to receive many small, incoming transfers of funds or to make deposits. Upon credit to the account, all or most of the transfers or deposits are wired to another account in a different geographic location in a manner inconsistent with the customer's business or history.
- Funds activity is unexplained, repetitive, or reveals unusual patterns.
- Payments or receipts are received that have no apparent link to legitimate contracts, goods, or services.
- Funds transfers are sent or received from the same person to or from different accounts.

Remote Deposit Capture

Remote deposit capture (RDC) is a product offered by banks that allows customers to scan a check and transmit an electronic image to the bank for deposit. This product offers increased convenience for customers because they no longer need to make a trip to the bank or an ATM to deposit checks. It is common for banks to allow individuals to deposit photos of checks taken with mobile phones. RDC decreases the cost to process checks for banks and is part of a gradual transition away from paper-based transactions. RDC is also increasingly used in correspondent banking, because it streamlines the deposit and clearing process. Correspondent banking is the provision of banking services by one bank to another bank.

The convenience provided by RDC can be abused by money launderers because they no longer need to go into the bank and risk detection. Money launderers who have RDC capabilities can move checks with ease through an account and possibly set up multiple imaging devices (e.g., multiple scanners and permitted mobile phones), enabling them to allow other criminals to process checks through the system. A money launderer might even arrange for someone else to set up an account and provide him with the ability to deposit checks. Without proper controls, RDC can also be misused to facilitate violations of sanctions requirements, for example, by processing transactions in a sanctioned country.

Although RDC can be used for money laundering, the more prominent risk relates to fraud. Because RDC minimizes human intervention in reviewing cleared items, it decreases the ability to identify potential fraud indicators, such as an altered check and multiple deposits of the same item. Often, the resulting fraud is not prevented but rather detected after it has already occurred.

To control the risks associated with RDC, efforts must be made to integrate RDC processing into other controls, such as monitoring and fraud-prevention systems. In fact, this integration should occur with any new product offered by an organization. This includes ensuring that items submitted via RDC are reviewed for sequentially numbered checks and money orders without payees, that the total volume of activity processed for an account via RDC is incorporated into the overall transaction monitoring system, that appropriate limits are placed on a customer's ability to deposit checks via RDC, that the product is offered to customers to whom it is appropriate, and that appropriate action is taken quickly when fraud is detected via RDC items.

Correspondent Banking

Correspondent banking is an arrangement whereby one bank acts as the agent of another bank in a foreign country. A local, or respondent, bank has customers who want banking services in a foreign country, so it contracts with a foreign correspondent bank to provide those services. By establishing multiple correspondent relationships, a local bank can undertake international financial transactions for itself and its customers in jurisdictions where it has no physical presence. Large international banks often act as correspondents for thousands of other banks.

The indirect nature of correspondent banking relationships means that the correspondent bank provides services for individuals and entities for which it has neither verified the identities nor obtained any firsthand knowledge.

The amount of money that flows through correspondent accounts can pose a significant threat, because the correspondent processes large volumes of transactions for the respondent's customers.

Correspondent banking is vulnerable to financial crime, especially because correspondent banks do not know the customers of the respondent directly and rely on the respondent bank's internal controls. In addition, less information is available to help the correspondent recognize suspicious activity.

Before establishing correspondent accounts, a bank should identify the respondent bank's owners and understand the nature of its regulatory oversight. According to the Wolfsberg Group, a bank's due diligence on a respondent bank should be based on the respondent's risk profile and the nature of the business relationship with that respondent bank. Due diligence should address specific risk indicators, such as the respondent bank's geographic risk, ownership and management structures, customer base, and products and services offered. Furthermore, the determination of the level and scope of due diligence that is required on a respondent bank should be made after considering the relationship between the respondent bank and its ultimate parent (if any). If the parent does not exercise substantial and effective control, due diligence should be conducted on both the respondent and the parent. The Wolfsberg Group has a Correspondent Banking Due Diligence Questionnaire that provides a standardized set of questions that can be used to perform due diligence.

Low-risk respondent banks might be offered a broad range of services, such as cash management—for example, interest-bearing accounts in a variety of currencies, international funds transfers, check clearing, payable-through accounts, and foreign exchange. High-risk respondent banks might be restricted to noncredit cash-management services.

The risks of correspondent banking include:

- The correspondent does not or cannot conduct typical due diligence to know the customers of the respondent (Know Your Customer's Customer).
- The correspondent does not have data on respondent transactions that typically enable transaction monitoring controls to identify unusual patterns.
- The correspondent can identify the respondent's regulators, but not always the degree of supervision to which the respondent is subject.
- The correspondent might have limited information on the respondent's anti-financial crime controls—perhaps through a questionnaire—yet still needs to rely on the respondent to have and use sufficient, effective controls on its customers.
- Some respondents are, themselves, correspondents to third banks, a practice called "nesting." Nested accounts further shield correspondent banks from knowing the parties involved.

Correspondent banking (Case example: Methods of money laundering)

In July 2020, the New York State Department of Financial Services (DFS) issued Deutsche Bank AG, its New York branch, and Deutsche Bank Trust Company Americas (collectively Deutsche Bank) a US$150 million penalty. DFS cited significant compliance failures in connection with the bank's relationship with disgraced American financier Jeffrey Epstein and its correspondent banking relationships, including those with Danske Bank Estonia (Danske) and FBME Bank.

In the case of Danske Bank Estonia and FBME bank, Deutsche Bank was found to have failed to monitor these banking clients, despite rating its

correspondent banking relationships with them both as high risk. Billions of dollars in suspicious transactions passed through Deutsche Bank's accounts and, in the case of Danske, significant flows were linked to money laundering by Russian oligarchs.

Deutsche Bank's internal compliance controls had flagged concerns with FBME as early as 2005 and with Danske Bank Estonia from the start of the relationship in 2007. However, these concerns did not result in timely actions to address the identified risks. In 2005 Deutsche Bank rated FBME bank as high risk, yet Deutsche Bank identified 826 suspicious transactions associated with FBME Bank after that rating.

FBME Bank declined to respond to Deutsche Bank's queries regarding the ultimate beneficial owners (UBOs) of FBME Bank's corporate clients. In one instance, the US authorities determined that the UBO was a Russian businessman associated with a Syrian military research and development organization. Deutsche Bank exited the relationship in 2014 after the Financial Crimes Enforcement Network (FinCEN) mandated all banks in the US to cease relationships with the bank.

Deutsche Bank was repeatedly warned of AML issues linked to nonresident accounts at Dankse Estonia, including those with links to Russia. In 2010 Deutsche Bank increased the risk score for the relationship with Dankse Estonia to the highest level, because it continued to see no improvements in the bank's nonresident portfolio. In 2013 and 2014, Deutsche Bank compliance staff recommended that the relationship be exited, but no action was taken until 2015.

Over US$150 billion was routed from Danske Bank Estonia through Deutsche Bank. Deutsche Bank identified 340 suspicious transactions linked to Danske Bank Estonia's US correspondent accounts with Deutsche Bank.

The DFS determined that Deutsche Bank's failures were caused by inadequate AML/CTF policies and procedures for its correspondent banking accounts. The correspondents failed to establish sufficiently specific criteria to trigger termination of relationships, provide practical guidance to staff on how to implement verification of respondents' UBOs, and act on identified red flags.

Key takeaways

- Senior management support is essential for compliance officers to effectively execute their duties.
- Organizations that ignore red flags associated with a customer relationship can suffer significant reputational, regulatory, and financial consequences.
- Nested accounts are high-risk because
    - Correspondent banks should include periodic reviews of their respondent bank's AML/CFT framework as part of their larger AML/CFT framework.
    - Correspondent banks need to undertake risk assessments and ensure that their policies and procedures regarding respondent bank relationships and their transactions are adequate to mitigate against identified risks, especially in high-risk relationships.

Payable-Through Accounts

In some correspondent relationships, the respondent bank's customers are permitted to conduct their own transactions—including sending wire transfers, making and withdrawing deposits, and maintaining checking accounts—through the respondent bank's correspondent account without first clearing the transactions through the respondent bank. Those arrangements are called payable-through accounts (PTAs).

In a traditional correspondent relationship, the respondent bank takes orders from its customers and passes them on to the correspondent bank. In these cases, the respondent bank has the ability to perform some level of oversight prior to executing the transaction. PTAs differ from typical correspondent accounts in that the foreign bank's customers have the ability to directly control funds at the correspondent bank.

PTAs can have a virtually unlimited number of subaccount holders, including individuals; commercial businesses; finance companies; exchange houses, or casas de cambio; and even other foreign banks. The services offered to subaccount holders and the terms of the PTAs are specified in the agreement signed by the correspondent and respondent banks.

PTAs held in the names of respondent banks often involve checks encoded with the bank's account number and a numeric code to identify the subaccount, which is the account of the respondent bank's customer. Sometimes, however, the identification of the subaccount holders is not given to the correspondent bank.

Elements of a PTA relationship that can threaten a correspondent bank's AML/CFT defenses include the following:

- PTAs with foreign institutions licensed in offshore financial service centers with weak or under-developed bank supervision and licensing laws
- PTA arrangements in which the correspondent bank regards the respondent bank as its sole customer and fails to apply its customer due diligence (CDD) policies and procedures to the customers of the respondent bank
- PTA arrangements in which subaccount holders have currency deposit and withdrawal privileges
- PTAs used in conjunction with a subsidiary, representative, or other office of the respondent bank, which might enable the respondent bank to offer the same services as a branch without being subject to supervision

Use of payable-through accounts (Case example: Methods of money laundering)

Payable-through accounts (PTA) are considered high risk because they can be used to facilitate money laundering, terrorist financing, and sanctions evasion. The misuse of PTAs significantly declined after many financial institutions implemented strict controls regarding their use by correspondent banking customers, based on individual and country risk. Organizations also established stringent processes and procedures concerning the scope and nature of permitted PTA activities, due diligence requirements, and associated disclosures. Recent cases of PTA misuse are rare, but an historical case provides a clear example.

Lombard Bank Ltd, a bank licensed by the South Pacific island of Vanuatu, opened a correspondent PTA at American Express Bank International (AEBI) in Miami, Florida. AEBI permitted the bank to have multiple authorized

signatures on the account. Lombard customers had no relationship with AEBI. However, Lombard offered its Central American customers nearly full banking services through its PTA at AEBI. The customers were even given checkbooks that allowed them to deposit and withdraw funds from Lombard's PTA.

This is how the misuse of PTAs worked: Lombard's PTA subaccount holders brought cash deposits to Lombard representatives in four Central American countries. Lombard couriers would then transport the cash to the bank's Miami affiliate, Lombard Credit Corporation, for deposit in the PTA at AEBI. Lombard customers also brought cash to the Lombard office in Miami, which was located in the same building as AEBI. That cash was also deposited in AEBI's PTA.

For two years, ending in June 1993, as much as US$200,000 in cash was received by Lombard's Miami affiliate on 104 occasions. AEBI did not know the source of the cash being deposited by Lombard's customers into the PTA. This fact raised significant AML/CFT compliance concerns related to KYC, due diligence, recordkeeping, and regulatory filing requirements.

In 1994, AEBI paid a multi-million-dollar fine for its connection to money laundering by a Mexican drug cartel. The organized crime group imported significant volumes of Colombian-origin drugs into the US and used AEBI's PTAs to launder the money.

Key takeaways

- PTAs often do not know the source of funds and customers' identities.
- Because PTAs can be offered to an unlimited number of subaccount holders, the exposure of correspondent banks to financial crime is very high.
- When correspondent banks offer PTAs, they should set clear limits on their use, depending on internal policies and the risk profile of the respondent.

Concentration Accounts

Concentration accounts are internal accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the bank, usually on the same day. They do this by aggregating funds from several locations into one centralized account (i.e., the concentration account). Concentration accounts are also known as special-use, omnibus, settlement, suspense, intraday, sweep, and collection accounts. They are frequently used to facilitate transactions for private banking, trust and custody accounts, funds transfers, and international affiliates.

Money laundering risks can arise in concentration accounts when the customer-identifying information, such as name, transaction amount, and account number, is separated from the financial transaction. When separation occurs, the audit trail is lost, and accounts can be misused or administered improperly.

Banks that use concentration accounts should implement adequate policies, procedures, and processes covering operation and recordkeeping for these accounts, including:

- Requiring dual signatures on general ledger tickets
- Prohibiting direct customer access to concentration accounts
- Capturing customer transactions in the customers' account statements
- Prohibiting customers' knowledge of concentration accounts and their ability to direct employees to conduct transactions through these accounts
- Retaining appropriate transaction and customer identification information
- Frequently reconciling accounts by an individual who is independent of the transactions
- Establishing a timely discrepancy-resolution process
- Identifying and monitoring recurring customer names

Private Banking

Private banking is an extremely lucrative and competitive global industry. Since the 2008 financial crisis, global regulators have placed greater scrutiny on private banks and their services.

Private banking provides highly personalized and confidential products and services to wealthy clients at fees that are often based on "assets under management." Private banking often operates semi-autonomously from other parts of a bank.

Fierce competition among private bankers for the high-net-worth individuals who are their main clientele has given rise to the need for tighter government controls worldwide. Competition brings increased pressures on relationship managers and marketing officers to obtain new clients, increase their assets under management, and contribute a greater percentage to the net income of their organizations. In addition, the compensation paid to most relationship managers in private banking is based largely on the assets under management that they bring to their organizations.

The following factors can contribute to the vulnerabilities of private banking to money laundering:

- Perceived high profitability
- Intense competition
- Powerful clientele
- High level of confidentiality
- Close trust developed between relationship managers and their clients
- Commission-based compensation for relationship managers
- Culture of secrecy and discretion developed by the relationship managers for their clients
- Role of relationship managers as client advocates to protect their clients
- Use of private investment companies by clients to reduce transparency of their beneficial owners

- Clients maintaining personal and business wealth in numerous jurisdictions, including offshore jurisdictions
- Clients' ability to utilize and control numerous legal entities for personal and family estate planning purposes

Private banking (Case example)

In 2015, the British regulator, the Financial Conduct Authority (FCA), fined Barclays global bank for AML/CFT violations. These regulatory breaches related to a £1.88 billion transaction that Barclays arranged and executed in 2011 and 2012 for several ultra-high net-worth customers. The customers involved were politically exposed persons (PEPs) and should therefore have been subjected to enhanced levels of due diligence and monitoring by Barclays. However, Barclays did not follow its standard policies and procedures. In fact, it applied a lower level of due diligence than was required for customers with lower risk profiles.

The FCA fined Barclays more than £72 million, which included the amount of revenue that Barclays generated from the transaction (£52 million) and penalties. On the date of the fine, it was the highest AML-related fine the FCA had ever issued.

Although the FCA concluded that the transaction was not linked to financial crime activity, it assessed the transaction as high risk due to the involvement of private banking, ultra-high net-worth customers, and PEPs, among other factors. High-risk transactions and customers require EDD measures, which Barclays failed to conduct. Barclays' policies and procedures required EDD. However, staff linked to the transaction did not follow them, and senior management failed to oversee the handling of the associated financial crime risks. Investigators claimed Barclay's sought profit over compliance, onboarding the clients as quickly as possible to generate £52.3 million in revenue.

Barclays did not obtain the necessary information from the customers to comply with financial crime requirements. Staff failed to establish the purpose and nature of the transaction and did not sufficiently corroborate the source of wealth and funds for the customers and transaction.

Barclays agreed to keep details of the transactions strictly confidential, even within the firm, and to compensate the customers up to £37.7 million if it failed to comply with these confidentiality restrictions. Few people knew of the existence and location of the firm's due diligence records, which were maintained in hard copy and not on Barclays' digital systems. This impacted how the customer relationship could be monitored on an ongoing basis and meant that Barclays could not respond promptly to the FCA's request for information.

The Barclays case exemplifies the fact that business interests should never take precedence over compliance with laws and regulations. The close relationships established in private banking often require a high degree of confidentiality. However, compliance checks should not be reduced or minimized. Strong AML/CFT compliance programs are successful only if organizations follow the policies and procedures that support them. Failure to follow regulations can lead to fines, even if no actual financial crime event occurred.

Key takeaways

- Business interests should never take precedence over compliance with laws and regulations.
- The close relationships established in private banking often require a higher degree of confidentiality, but this should not reduce or minimize the required compliance checks.
- Strong AML/CFT compliance programs need organizations to follow the policies and procedures that support them.
- Failure to follow a robust compliance plan can lead to fines, even if no actual financial crime event occurred.

Use of Private Investment Companies in Private Banking

In offshore and international financial centers, private banking customers are often nonresidents; that is, they conduct their banking in a country other than the one in which they reside. Their assets might move overseas, where they are held in the name of corporate vehicles such as private investment companies (PICs) established in secrecy havens. PICs are corporations established by individual bank customers and others in offshore jurisdictions to hold assets. They are shell companies formed to maintain clients' confidentiality and serve various tax- and trust-related purposes. PICs have been an element of many high-profile laundering cases because they are effective laundering vehicles.

The secrecy laws of the offshore havens where PICs are often established can conceal the true identities of customers' beneficial owners. As an additional layer of secrecy, some PICs are established by company formation agents with nominee directors who hold titles to companies for the benefit of individuals. These beneficial owners could remain undisclosed and sometimes are subject to attorney-client privilege and other similar legal safeguards. Many private banks establish PICs for their clients, often through an affiliated trust company in an offshore secrecy haven. Criminals can establish complex shell company networks in which a company registered in one offshore jurisdiction might be linked to companies and accounts in other jurisdictions.

Use of PICs in private banking (Case example: Methods of money laundering)

In 2014, Israeli-based Bank Leumi admitted that it had assisted more than 1,500 US taxpayers in hiding their assets in Bank Leumi's offshore affiliates in Switzerland and Luxembourg. According to reports, for several years Bank Leumi sent private bankers to the United States to meet with its US clients to discuss their offshore portfolio and tax-mitigation strategies. As part of this strategy, the bank assisted in organizing nominee corporate entities registered in Belize and other offshore jurisdictions to hide their clients' private offshore accounts and maintained several US clients' accounts under

assumed names or numbered accounts. Bank Leumi also provided "hold mail" services and offered loans to its US clients that were collateralized by their offshore assets, which were not declared to US tax authorities.

As a result of the settlement, Bank Leumi was assessed US$270 million in fines and ordered to cease providing private banking and investment services for all US clients and accounts with US beneficial owners. This settlement led to Bank Leumi selling its affiliates Bank Leumi Private Bank and Bank Leumi (Luxembourg).

Key takeaways

- Nominee corporate entities registered in high-risk offshore jurisdictions are an attractive vehicle for evading tax obligations.
- Care should be taken when dealing with assets associated with non-nationals to reduce the risk of them being moved or placed to deliberately avoid tax.
- Facilitating tax evasion is a serious offense that can lead to large fines and negatively impact a regulated firm's ability to do business with certain customers and jurisdictions.

Politically Exposed Persons

According to FATF, there are three types of politically exposed persons (PEPs).

1. **Foreign PEPs:** Individuals who are or have in the past been entrusted with prominent public functions by a foreign country (e.g., heads of state or of government; senior politicians; senior government, judicial, and military officials; senior executives of state-owned corporations; and important political party officials).
2. **Domestic PEPs:** Individuals who are or have in the past been entrusted domestically with prominent public functions (e.g., heads of state or of government; senior politicians; senior government, judicial, and military

officials; senior executives of state-owned corporations; and important political party officials).

3. **International organization PEPs:** Individuals who are or have in the past been entrusted with a prominent function (e.g., managing director, secretary general, executive director, chairperson, and president) by an international organization, such as the United Nations' six principal organs and multiple specialized agencies, the IMF, the World Bank, the North Atlantic Treaty Organization, and the Organization of American States (OAS), among many others.

Relatives and close associates of PEPs are also considered to be PEPs. The definition of PEPs is not intended to cover middle ranking and more junior individuals in the above categories.

PEPs have been the source of problems for several regulated organizations, particularly with regard to reputational risk, as the following examples show:

- **Eldar Mahmudov:** The former minister of national security of Azerbaijan from 2004 to 2015, Mahmudov accumulated substantial real estate holdings in the UK, Spain, Luxembourg, Lithuania, and Cyprus, many of them in his children's names. Investigative journalists estimate his total worth at over €100 million. The majority of his assets are held by the ex-official's son and daughter.
- **ABLV Bank:** In 2018, the Latvian bank was identified by FINCEN as a financial institution of primary money laundering concern, pursuant to Section 311 of the USA PATRIOT Act. According to FINCEN, it had facilitated money laundering for years on behalf of corrupt government officials and other PEPs from Azerbaijan, Russia, and Ukraine, namely by funneling billions of dollars in the proceeds of corruption and asset stripping through shell company accounts.
- **Najib Razak:** The former prime minister of Malaysia (2009-2018) was convicted of abuse of power and money laundering in July 2020 and sentenced to 12 years in prison. He was found guilty of having been the primary beneficiary of large-scale embezzlement at 1Malaysia Development Berhad (1MDB), a state-owned development bank. Billions of dollars were fraudulently withdrawn from 1MDB to fund purchases of high-end real estate and luxury goods, and to make investments through various shell firms.

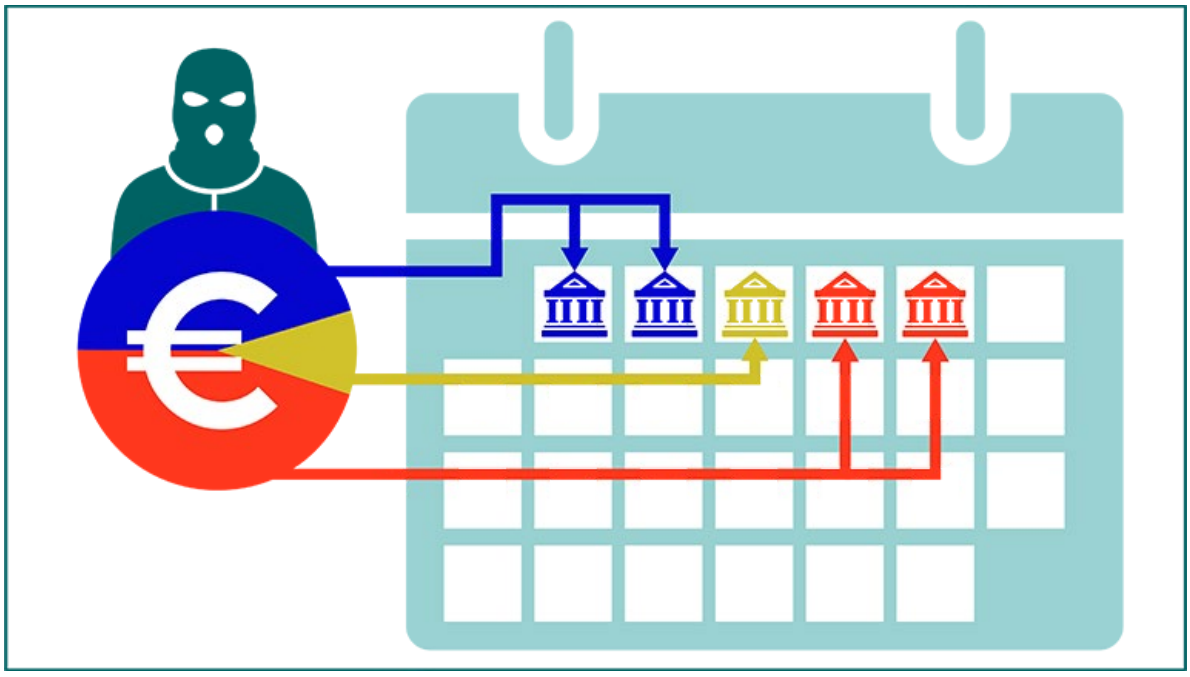
- **Diezani Alison-Madueke:** The former Nigerian minister of petroleum resources was accused of siphoning off billions of dollars from Nigerian states' coffers. In 2017, the US Department of Justice seized US$145 million worth of properties controlled by Alison-Madueke, including a US$50 million apartment in New York City and an US$80 million yacht.
- **Riad Salameh:** In 2021, Switzerland, France, and Luxembourg opened criminal investigations into Lebanon's long-standing central bank governor. In 2020, investigative media reported on Salameh's more than US$100 million worth of domestic and overseas assets. In one example, a company tied to the governor bought a stake in his son's wealth-management business and later sold it for a profit to a Lebanese bank under Salameh's supervision.
- **Lai Xiaomin**: In 2021, former chairman (2012-2018) of Huarong, one of China's largest state-controlled asset-management firms, was sentenced to death by a Chinese court for accepting US$227 million in bribes and associated money laundering. He had allegedly invested a portion of the proceeds in gold bars and luxury cars, and made large deposits into his mother's bank account.
- **Petrobras:** A global commodities trader agreed in 2020 to pay US$135 million to resolve a US Department of Justice investigation into a long-running bribery scheme in Latin America. The scheme involved kickbacks to senior executives at Petrobras, Brazil's national oil company, in exchange for confidential pricing and competitor information. Bribes were paid under fraudulent consulting agreements by and to shell companies, using fake invoices and offshore accounts.
- **Alexander Shestun:** A Russian court in 2020 sentenced the former head of Serpukhov District in the Moscow region to 15 years in prison. The court seized 106 real estate properties, 642 land plots, seven vehicles, precious metals, collection coins, and cash from bribes paid to Shestun by the local business community.

Structuring

Designing a transaction to evade triggering a reporting or recordkeeping requirement is called *structuring*. Structuring is one of the most common money laundering methods. It is a crime in many countries and must be reported by filing a suspicious activity report (SAR). The individuals engaged in structuring may be "runners" hired by the launderers, that is, individuals who travel from bank to bank depositing cash and purchasing monetary instruments in amounts under reporting thresholds.

Structuring can be done in many settings and industries, including banking, money services businesses, and casinos. "Smurfing" is a common structuring technique that involves multiple individuals making multiple cash deposits and/or buying multiple monetary instruments or bank drafts in amounts under the reporting threshold to evade detection.

Cash structuring example



Structuring is one of the most commonly reported forms of unusual activity. Well-known examples of structure include:

- **A customer breaks a large transaction into two or more smaller transactions.**

  Henri wants to conduct a transaction involving $18,000 in cash. However, knowing that depositing it all at once would exceed his country's cash-reporting threshold of $10,000 and trigger the filing of a currency transaction report, he goes to three different banks and deposits $6,000 in each.

- **A large transaction is broken into two or more smaller transactions that are conducted by two or more people.**

  Jennifer wants to send a $5,000 money transfer. Knowing that in her country there is a threshold of $3,000 for the recording of funds transfers, she sends a $2,500 money transfer and asks her friend to send another $2,500 money transfer.

- **An individual sends his fortune to another country.**

  Mr. Lee, a wealthy Chinese businessman, sends his gained wealth of US$1 million in sums of US$40,000 via friends and business contacts to a British bank in London. The reason he does not deposit it into his own bank account in London is that the Chinese government has currency controls in place for transactions over US$50,000 abroad.

Foreign money brokers structure transactions by following these steps:

1. A structurer, who is acting for a foreign money broker, opens several checking accounts in country A using real and fictitious names. Sometimes the structurer uses identification documents of deceased people supplied by the money brokers.
2. With funds supplied by the money brokers, the structurer opens the accounts with inconspicuous amounts, usually in the low four figures.
3. To allay bank suspicions, the money brokers sometimes deposit extra funds to cover their living expenses and make the accounts appear legitimate.
4. Once the accounts are opened, the structurer signs the newly issued checks, leaving the payee, date, and amount lines blank.
5. The structurer sends the signed blank checks to the money broker in country B, usually by courier.

6. A structurer might open as many as two dozen checking accounts in this fashion. It is not uncommon for brokers to have more than 20 of these checking accounts in country A available at any given time.
7. The checking accounts usually accumulate only a few thousand dollars before they are cleared out by checks drawn by the money brokers to pay for exports from country A to country B's money brokerage customers.
8. The availability of hundreds of these accounts to country B's money brokers leaves open the possibility that tens of millions of dollars could pass through them each year.

Structuring (Case example: Methods of money laundering)

In June 2018, Commonwealth Bank (CBA) agreed to pay a AUD700 million settlement plus legal costs. At the time, this was the highest penalty in Australian corporate history for breaches of AML/CFT laws. The Australian Transaction Reports and Analysis Centre (AUSTRAC) accused the bank of serious systemic failures to report suspicious deposits, transfers, and accounts. Those failures allowed millions of dollars to be laundered on behalf of drug importers through a method known as structuring. Structuring is the illegal act of splitting cash deposits or withdrawals into smaller amounts, or purchasing monetary instruments, to stay under a currency reporting threshold. Money launderers use structuring to avoid triggering a filing by a financial institution.

In Australia, banks are required to file threshold transaction reports (TTRs) to AUSTRAC for transactions of AUD10,000 or more within 10 business days. CBA failed to report over 53,000 transactions that were run through intelligent deposit machines (IDMs) from 2012 to 2015. IDMs are a form of ATM that accepts cash and check deposits. These deposits are automatically counted, credited into CBA accounts, and made available for immediate transfer, domestically and internationally. AUSTRAC alleged that CBA did not limit the number of transactions a customer could make per day; its IDMs allowed up to 200 bills per transaction. A criminal who inserted AUD100 bills could deposit up to AUD20,000 in one transaction, which is well above the mandatory reporting limit.

IDMs also allow anonymous cash deposits. A card from any financial institution could deposit funds into a CBA account. That means a criminal could potentially deposit millions of dollars through a machine in one day anonymously. Because the money appears instantly, a user could immediately transfer the money to another account, including an offshore account.

In May and June 2016, more than AUD1 billion in cash moved through CBA's IDMs. Many of the transactions were deposited in amounts that fell below the threshold transaction limit.

Prior to using IDMs, CBA did not carry out an AML/CFT risk assessment. Despite an exponential rise in cash deposits and alerts raised by its internal transactional monitoring system, CBA did not conduct a subsequent risk assessment.

In addition, CBA breached its obligation to perform checks on 80 suspicious customers. Even when structuring was suspected on CBA accounts, the institution failed to monitor these customers and conduct EDD, as required when a suspicion is formed.

Key takeaways

- Structuring can involve many channels, such as IDMs.
- Adequate controls must be in place to ensure proper monitoring and reporting.
- New technologies need to be critically assessed for AML/CFT risks.
- Organizations need to limit the number of customers' daily transactions and the number of bills per transaction.

Microstructuring

Microstructuring is another method of placing large amounts of illicit cash into the financial system. It is essentially the same concept as structuring, although it is done at a much smaller level. Instead of taking $18,000 and breaking it into two deposits to evade reporting requirements, the microstructurer breaks it into 20 deposits of approximately $900 each, making the suspicious activity extremely difficult to detect.

In the case of a Colombian drug cartel, the cash proceeds of US drug sales were deposited into accounts in New York with linked ATM cards, which were provided to associates in Colombia. Deposits were made on a regular schedule, with the Colombian associates withdrawing the funds as they were deposited and giving them to the drug lords. In one case in New York, an individual was trailed by law enforcement authorities as he went from bank to bank in Manhattan. When they stopped him, he had US$165,000 in cash.

Microstructuring red flags include:

- The use of counter deposit slips instead of preprinted deposit slips
- Frequent activity in an account immediately following the opening of the account with only preliminary and incomplete documentation
- Frequent visits to make cash deposits of nominal amounts that are inconsistent with typical business or personal banking activity
- Cash deposits followed by ATM withdrawals, particularly in high-risk countries
- Cash deposits made into business accounts by third parties with no apparent connection to the company

Credit Unions and Building Societies

Credit unions, which are also known as building societies in some jurisdictions, are not-for-profit member-owned-and-operated democratic financial cooperatives.

Credit unions do not have clients or customers; rather, they have members who are also owners. Credit unions serve only the financial needs of their members and are governed by a "one-member, one-vote" philosophy. A member must purchase an initial capital share of the credit union, permitting him to access the products and services offered by the credit union. Credit union membership is based on a common bond, a linkage shared by savers and borrowers who belong to a specific community, organization, religion, or place of employment.

Credit unions can vary significantly in both size and complexity. Some credit unions have a few hundred members, and others have hundreds of thousands of members with tens of billions of dollars in assets under management. Some credit unions focus on meeting only a few niche needs of their members, while others offer a full suite of products and services to rival most retail banks.

Most credit unions focus primarily on servicing personal banking relationships from within their community. Depending on their member eligibility model, some also facilitate memberships for small-to-medium-sized corporate and entity account holders, although credit unions are prohibited from doing so in some jurisdictions. Generally, credit unions do not participate in trade-based financing, facilitate correspondent banking relationships, or maintain large corporate relationships, particularly those with international banking needs.

In many jurisdictions, credit unions rely on credit union centrals for a variety of services. A credit union central is best defined as a trade association for credit unions; it is owned by its member credit unions and helps to serve many of their financial needs. Services might include those related to capital liquidity; research, training, and advocacy with respect to regulatory obligations; shared operational and back-office processes, such as check clearing; and electronic funds transfer (EFT) processing. In general, they help to negotiate shared contracts for common services, allowing many smaller credit unions to leverage economies of scale that they would not otherwise be able to do.

With respect to regulatory requirements and oversight, credit unions operate very similarly to banks in most jurisdictions. They have capital, liquidity, risk-

management, recordkeeping, and reporting obligations similar to banks, although there might be minor differences between institutions that are subject to the oversight of regional versus federal regulators and regulations. Because credit unions are included under FATF's definition of a financial institution, national AML/CFT regimes that follow FATF's recommendations treat credit unions similarly to banks.

The United Kingdom's Joint Money Laundering Steering Group (JMLSG) states in its sectoral guidance that credit unions potentially pose lower money laundering and terrorist financing risks, because they typically have a restricted or localized customer base and offer fewer products and services, with more limitations, than retail banks. Credit unions are also less exposed to third-party transfers. However, the guidance notes that, while their limited functionality and flexibility makes them lower risk for money laundering, these restrictions might not fully deter potential terrorist financiers.

The guidance elaborates on how a risk-based approach should be considered for credit unions and lists potential risk indicators to take into consideration. One risk factor highlighted is adult parents or guardians who use a child's account to launder funds. Other risk factors include allowing transfers to or from third parties; frequent cash payments; customers engaging in large one-time transactions; unusual loans or savings transactions (e.g., early repayment of a loan from an unknown income source); and reluctance from a customer to provide evidence of identity or information about the purpose or nature of the business relationship.

Given the services offered by credit unions and their connections to employers, benefits providers, and schools, it is important to consider whether a customer might have a reasonable explanation for not having suitable ID and whether they might be considered "financially excluded," i.e., unable to access the traditional banking system. The guidance provides examples, such as a letter from the employer or school, which can help to identify someone who is financially excluded.

Ongoing monitoring can potentially be easier for credit unions, especially if they are smaller, because there is a narrower range of expected activity to monitor against, and transactions are often processed manually, making it easier to identify unusual activity. Additionally, smaller credit unions have fewer organizational hurdles to overcome when reporting suspicious activity to the nominated officer.

Nonbank Financial Institutions

Credit Card Industry

The credit card industry includes:

- Credit card associations, such as American Express, MasterCard, and Visa, which license member banks to issue bank cards, authorize merchants to accept those cards, or both
- Issuing banks, which solicit potential customers and issue the credit cards
- Acquiring banks, which process transactions for merchants who accept credit cards
- Third-party payment processors (TPPP), which contract with issuing and acquiring banks to provide payment-processing services to merchants and other business entities, typically initiating transactions on behalf of merchant clients that do not have a direct relationship with the TPPP's financial institution

Credit card accounts are not typically used in the initial placement stage of money laundering, because the industry generally restricts cash payments. They are more likely to be used in the layering and integration stages.

Examples

- Money launderer Josh prepays his credit card using illicit funds that he has already introduced into the banking system, creating a credit balance on his account. Josh then requests a credit refund, which enables him to further obscure the origin of the funds. This constitutes layering. Josh then uses the illicit money he placed in his bank account and the credit card refund to pay for a new kitchen. Through these steps, he has integrated his illicit funds into the financial system.
- A money launderer places his illegal funds in accounts at offshore banks and then accesses the funds using credit and debit cards associated with the offshore account. Alternatively, he smuggles the cash out of one country into an offshore jurisdiction with lax regulatory oversight, places

the cash in offshore banks, and accesses the illicit funds using credit or debit cards.

- In a report entitled *Extent of Money Laundering through Credit Cards Is Unknown*, the US Government Accountability Office, the US Congressional watchdog, offers the following hypothetical money laundering scenario using credit cards: "Money launderers establish a legitimate business in the US as a 'front' for their illicit activity. They establish a bank account with a US-based bank and obtain credit cards and ATM cards under the name of the 'front business.' Funds from their illicit activities are deposited into the bank account in the United States. While in another country, where their US-based bank has affiliates, they make withdrawals from their US bank account, using credit cards and ATM cards. Money is deposited by one of their cohorts in the US and is transferred to pay off the credit card loan or even prepay the credit card. The bank's online services make it possible to transfer funds between checking and credit card accounts."

Third-Party Payment Processors

TPPPs are generally bank customers that provide payment-processing services to merchants and other business entities. They often use their commercial bank accounts to conduct payment processing for their merchant clients. Often, they are not subject to AML/CFT requirements.

TPPPs traditionally contracted with US retailers (i.e., merchants) that had physical locations in the United States in order to help collect monies owed by customers. These merchant transactions primarily included credit card payments, but they also covered ACH debits and creating and depositing remotely created checks (RCCs) and demand drafts. With the expansion of the internet, TPPPs can now service a variety of domestic and international merchants, including conventional retail and internet-based establishments, as well as prepaid travel and internet gaming enterprises. Considering the expansion of services and the fact that a financial organization maintains a relationship with the TPPP and not the underlying merchant, it becomes difficult for the financial organization to know on whose behalf it is processing a transaction.

The types of merchants to which a TPPP provides its payment-processing services can increase the TPPP's vulnerability to money laundering, identity

theft, fraud, and other illegal activities. For example, TPPPs that provide services to telemarketing, gambling (e.g., online and physical casinos), and internet merchants, as well as those that process RCCs for these entities, might present a high level of risk to a financial organization, because they carry a high risk for consumer fraud and money laundering.

Examples of risks posed by TPPP include the following:

- **Multiple financial organization relationships:** The TPPP might maintain relationships at multiple organizations, which hinders the organizations' ability to know the entire customer relationship. This arrangement is purposeful by TPPPs engaged in suspicious activity to limit the financial organizations' ability to recognize suspicious activities and exit the relationships.
- **Money laundering:** TPPPs can be used by criminals to mask transactions and launder the proceeds of crime. One way to engage in money laundering through a TPPP is to send funds directly to a financial organization from a foreign jurisdiction through an international ACH payment. Given the significant number of transactions conducted through a TPPP, this activity might not be identified.
- **High return rates from unauthorized transactions:** TPPPs engaged in suspicious activity, and those being used by criminals might have higher than average return rates related to unauthorized transactions. At the merchant level, the criminal merchant might have acceptable return rates compared to the percentage of the TPPP's total transaction volume, but when compared with individual originators, the return rate will be significantly higher.

It is important to understand that credit card transactions, whether conducted through a TPPP or other financial organization, do not need to be significant in amount to be considered suspicious or unusual. For example, there might be a high number of small dollar transactions, repeat customers or donors with no discernible pattern, and customers who receive international donations or other payments that do not match the information provided by the customer when they described their business or the customer's historical activity. Therefore, it is important to have strong CDD, EDD, and transaction monitoring controls to detect suspicious activity and customers that fall outside an organization's risk appetite.

Money Services Business

A money services business (MSB) or money or value transfer service (MVTS), as defined by FATF, transmits or converts currencies. These businesses typically provide currency exchange, money transmission, check-cashing services, and money order services.

MSB laws vary by jurisdiction. For example, in the United States, FinCEN defines MSB as any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities:

- **Dealer in foreign exchange:** These MSBs provide currency exchange services (e.g., US dollars converted to euros). They typically operate along international borders, in airports, and near communities with high populations of foreign individuals.
- **Check casher:** Check-cashing services can be offered by retail businesses or as standalone operations. Depending on the model, the MSB might cash checks for consumers and commercial businesses. In addition to check cashing, these MSBs might provide additional financial services so their customers can pay bills, purchase money orders, and transmit funds domestically and internationally.
- **Issuer of traveler's checks or money orders:** The issuer of a money order or traveler's check is responsible for the payment of the item and often uses agents to sell the negotiable items.
- **Money transmitter:** Money transmitters accept currency and funds for the purpose of transferring those funds electronically through a financial agency, institution, or EFT network. Money transmitters also include certain business models involving money transmission denominated in value that substitutes for currency, specifically, convertible virtual currencies (CVCs). Examples of well-known money transmitters are Western Union, MoneyGram, PayPal, and Coinbase.
- **Provider and seller of prepaid access:** Providers of prepaid access arrange for access to funds or to the value of funds that have been paid in advance. These funds can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification

number. Prepaid access is also referred to as stored value. Prepaid access can be open loop or closed loop.

  - **Open-loop prepaid cards** can be used for purchases at any merchant that accepts cards issued for use on the payment network associated with the card. They can also be used to access cash at any ATM that connects to the affiliated ATM network. Open-loop prepaid cards usually are branded with the network logo, such as American Express, Visa, or MasterCard.
  - **Closed-loop prepaid cards** are typically limited to buying goods or services from the merchant issuing the card.

- **US Postal Service:** Because the US Postal Service sells its own money orders, it is considered to be an MSB.

FinCEN published a Final Rule in 2012 to expand the definition of MSB to detail when an entity qualifies as an MSB based on its activities within the United States, even if none of its agents, agencies, branches, or offices is physically located there. The Final Rule arose in part from the recognition that the internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations. Absent an exception, MSBs are required to register with FinCEN. FinCEN issued additional interpretive guidance consolidating current FinCEN regulations and related administrative rulings. FinCEN applied these rules and interpretations to other common business models involving CVCs engaged in the same underlying patterns of activity.

MSBs in Canada are defined as businesses engaged in foreign exchange dealing; money transferring; and cashing and selling money orders, traveler's checks, and similar monetary instruments to the public. These MSBs are required to register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

MSBs can range from small, independent businesses to large multinational organizations. Organizations can either provide MSB services as their primary business or as an ancillary service to primary retail store operations. Businesses that provide ancillary MSB services typically include grocery stores, drug stores, restaurants, and bars. The services provided by these businesses include, but are not limited to, cashing payroll checks and selling prepaid cards. Although many of these businesses have brick-and-mortar locations,

the number of MSBs operating solely on the internet with no physical presence or a network of agents is increasing.

Traditional MSBs typically provide services to the underserved or unbanked individuals. The focus on this market leads them to locate their operations in regions with limited or no banking services. Additionally, they typically provide lower cost services compared with financial institutions for certain service offerings. For example, engaging in domestic or international wire transfers through a financial institution can be time consuming and costly for a consumer. Conducting similar transactions through an MSB can occur quickly and at a much lower cost. Additional services could include bill payments, payday lending, and commercial check cashing.

MSBs can be categorized into principals or agents. Principals primarily provide MSB services and act as the issuers of money orders and traveler's checks or the providers of money transmission. In the United States, principal MSBs are required to have written AML policies, procedures, and internal controls; appoint a BSA officer; provide education and training; conduct independent reviews and audits; and monitor transactions for suspicious activity.

Agents are entities that seek to provide MSB-type services in addition to their existing products and services. An agent could be a principal MSB because it offers check cashing as its primary service but an agent because it provides money-transmission services through a principal money transmitter MSB. For agents to use money-transmission services, they must enter into an agent service agreement with a principal MSB. An additional byproduct of the principal-agent relationship is that it allows principal MSBs to expand their business and reach a wider customer market without the need for added overhead. Agents of a principal MSB are required to follow the same state and federal regulations as a principal MSB (e.g., AML/CFT procedures and suspicious activity monitoring).

Examples of how MSBs can be used by criminals include:

- Fraud in the healthcare industry is rising. Healthcare businesses, such as home healthcare companies, might engage in fraudulent practices by presenting checks derived from fraud to check cashers that they know will not ask for proof of the payee's identity, will either not file or file false currency transaction reports (CTRs), and will not report them to the government for engaging in suspicious activity. The check casher can be compromised by an employee insider or attempt to be business-friendly

by avoiding complying with legal or regulatory requirements that are considered to be burdens to its customers.

- Criminals obtain low-cost workers' compensation insurance policies by grossly deflating payroll amounts. After securing certificates of insurance, organizers rent the certificates to other individuals and businesses for a fee. Because the policies are obtained fraudulently, employees are not covered and are therefore left vulnerable to high medical costs when they incur an on-the-job injury. The payroll amounts are then concealed by cashing checks at an MSB that circumvents proper bookkeeping measures. The criminal makes a significant amount of money to the detriment of workers.
- Money launderers use money remitters and currency exchanges to make funds available to criminal organizations at a destination country in the local currency. The launderer or broker then sells the criminal dollars to foreign businesspeople wishing to make legitimate purchases of goods for export.

It is a common misconception that there is minimal oversight of the MSB industry. In fact, many MSBs are overseen by a variety of national and/or local regulators and often maintain compliant AML/CFT programs. In addition, they are monitored by the banks with which they maintain relationships. However, the scrutiny applied to MSBs can vary significantly, in large part due to the ease with which some MSBs can establish their business. Additionally, many MSBs are small (i.e., one-store operators) and might not have robust AML/CFT programs compared with their larger national counterparts. For this reason, one of the most important aspects of due diligence for a bank that is establishing a relationship with an MSB is to confirm that the MSB has implemented a sufficient AML/CFT program (e.g., procedures, training, and suspicious activity monitoring) and is properly licensed and/or registered in the jurisdictions in which it operates.

Use of MSBs (Case example: Methods of money laundering)

Nonbank financial services, such as money services businesses (MSBs) provide valuable services to facilitate remittances, conduct money changing and foreign exchange activities, support areas that are underserved by the banking sector, and promote financial inclusion for individuals who have limited access to the formal banking system. However, the cash-intensive nature of MSBs and the transactional nature of their relationships with customers make this service attractive to financial criminals for moving illicit funds.

The Anti-Money Laundering Council (AMLC), the Philippines' financial intelligence unit, cited MSBs as high risk in facilitating criminal proceeds in its 2021 National Risk Assessment, particularly in relation to drug trafficking and child and sexual exploitation. It highlighted that the frequent use of cash poses a threat in concealing the source of funds and its potential associated links to unlawful activities.

AMLC's statement followed the US$81 million Bangladesh Bank Heist in 2016, in which three MSBs, including Philrem Service Corp. (Philrem), facilitated the movement of money from the heist via remittances from fictitious accounts to casinos in the Philippines. This incident drove increased scrutiny from the regulators on the risks posed by such entities and led to a more proactive supervisory stance.

In 2016, the financial regulator Bangko Sentral ng Pilipinas (BSP), in its campaign to combat illegal money movement via MSBs, revoked the licenses of three MSB companies, due to "significant violations" in AML compliance. Among them was Philrem; it's licenses to offer services as a foreign exchange dealer, money changer, and remittance agent were subsequently revoked.

AML rules and regulations covering MSBs such as Philrem have been in place since 2011 in the Philippines and require MSBs to comply with the same requirements as banks, such as risk assessments, CDD, and transaction monitoring. The BSP and AMLC have since implemented new measures to combat the risks of facilitating illegal proceeds via MSBs, including a restructure and consolidation of the sector to strengthen its framework for AML/CTF compliance.

In the Philippines, the fragmented nature of the MSB industry and its smaller size means that principals and agents often lack appropriate resources and experience and that, as a result, the understanding of the financial crime risks associated with the sector is still developing.

Key takeaways

- MSBs must comply with the same AML requirements as banks.
- Small MSBs might lack resources and experience, leading to compliance issues.
- The cash-intensive and transactional nature of MSBs can facilitate money laundering.
- MSBs offer valuable services and are important for financial inclusion.

Insurance Companies

The insurance industry provides risk transfer, savings, and investment products to a variety of consumers worldwide, ranging from individuals to large corporations to governments. An important aspect of the way the insurance industry operates is that most of the business conducted by insurance companies is transacted through intermediaries, such as agents and independent brokers. Insurers, with some exceptions, are subject to AML requirements.

The susceptibility of the insurance industry to money laundering is not as high as that for other types of financial organizations. For example, policies for property, casualty, title, and health insurance typically do not offer investment features, cash buildups, the option to transfer funds from one to policy another, or other means of hiding and moving money. However, certain sectors of the insurance industry, such as life insurance and annuities, are a primary target of criminals who engage in money laundering and terrorist financing. In several ways, the sector's vulnerability to money laundering is similar to that of the securities sector; in some jurisdictions, life insurance policies are even viewed as investment vehicles similar to securities.

According to FATF, life insurance is by far the most attractive area of the insurance sector to money launderers. Substantial sums can be invested in

widely available life insurance products, and many feature a high degree of flexibility, while at the same time ensuring nonnegligible rates of return. Many life insurance policies are structured to pay a fixed dollar amount upon the death of the insured party. In contrast, other life insurance products, such as whole and permanent life insurance, have an investment value, which can create a cash value above the original investment when the policyholder cancels it. Such characteristics are of considerable value to honest policyholders, but they also offer money launderers opportunities to legitimize their illicit funds. Furthermore, the most frequently observed individual typology relates to international transactions, demonstrating the cross-border reach of insurance-related money laundering operations.

For criminals seeking to launder funds, life insurance products with no cash surrender value are the least attractive. Products that feature payments of cash surrender value and the opportunity to nominate beneficiaries from the first day of the policy are the most attractive and therefore higher risk.

Annuities are another type of insurance policy with cash value. An annuity is an investment that provides a defined series of payments in the future in exchange for an up-front sum of money. Annuity contracts can allow criminals to exchange illicit funds for an immediate or deferred income stream, which typically takes the form of monthly payments starting on a specified date. In both cases, a policyholder can place a large sum of money into a policy with the expectation that it will grow based on the underlying investment, which can be fixed or variable. Unit-linked policies and insurance wrappers are also high-risk insurance products because of their high value accumulation and flexibility in adding and managing assets.

Typical features of high-risk insurance products include:

- Offers the ability to fold funds and assets into the policy
- Full or partial underlying investments under the control of the customer
- Can offer the option of asset transfers
- Can have a high upper limit for the amount of funds held

Another indicator of possible money laundering in the insurance industry is when a potential policyholder is more interested in a policy's cancellation terms than its benefits.

Vulnerabilities in the insurance sector include the following:

- **Lack of oversight/controls over intermediaries:** Insurance brokers have a great deal of control and freedom regarding policies.
- **Decentralized oversight over aspects of the sales force:** Insurance companies can have employees (i.e., captive agents) who are subject to the full control of the insurance company. Noncaptive agents offer an insurance company's products, but they are not employed by an insurance company. They often work with several insurance companies to find the best mix of products for their clients and may "fall between the cracks" of multiple insurance companies. Agents who are complicit with money launderers might work to find the company with the weakest AML oversight.
- **Sales-driven objectives:** The focus of brokers is on selling the insurance products; therefore, they might overlook signs of money laundering, such as a lack of explanation for wealth and unusual methods for paying insurance premiums.

  Examples of how money can be laundered through the insurance industry include:

- Certain insurance policies operate in the same manner as unit trusts or mutual funds. The customer can overfund the policy and move funds into and out of the policy while paying early withdrawal penalties. When such funds are reimbursed by the insurance company (e.g., by check), the launderer has successfully obscured the link between the crime and the generated funds.
- The purchase and redemption of single premium insurance bonds are key laundering vehicles. The bonds can be purchased from insurance companies and then redeemed prior to their full term at a discount. In such cases, the balance of the bond is paid to a launderer in the form of a sanitized check from the insurance company.
- A free-look period is a feature that allows investors—for a short period of time after the policy is signed and the premium paid—to back out of a policy without penalty. This process allows the money launderer to receive an insurance check, which represents cleaned funds. However, as more

insurance companies are subject to AML program requirements, this type of money laundering is more readily detected and reported.

- One indicator of possible money laundering is when a potential policyholder is more interested in the cancellation terms of a policy than the benefits of the policy. The launderer buys a policy with illicit money and then tells the insurance company that he has changed his mind and does not need the policy. After paying a penalty, the launderer redeems the policy and receives a clean check from a respected insurer.

The FATF *Money Laundering Typologies* report provides some additional typologies related to the insurance industry:

- Third parties that fund insurance policies (i.e., not the policyholder) have not been subject to regular identification procedures when the insurance contract was concluded. The source of funds and the relationship between policyholder and the third party might be unclear to the insurance company.
- Some customers actually do not seek insurance coverage; rather, it is an investment opportunity. Money laundering is enabled by using large sums of money to make substantial payments into single-premium life insurance policies, which serve as wrapped investment policies. A variation on this method is the use of large premium deposits to fund annual premiums. Such policies, which are comparable to single-premium policies, also enable the customer to invest substantial amounts of money with an insurance company. Because the annual premiums are paid from an account that must be funded with the total amount, a life insurance product with apparently lower money laundering risk will bear the features of the higher risk single-premium policy.

In the insurance sector, most of the business is conducted through intermediaries. As a result, often it is the intermediaries' application of AML regulatory requirements that is unsatisfactory.

When an insurance company assesses money laundering and terrorist financing risks, it must consider whether it permits customers to:

- Use cash or cash equivalents to purchase insurance products
- Purchase an insurance product with a single premium or lump-sum payment
- Borrow money against an insurance product's value

Securities Broker-Dealers

The securities industry provides opportunities for criminals to engage in money laundering and terrorist financing anonymously, given the varying levels of AML program requirements in different types of businesses and the high volume of transactions. The world's capital markets are vast in size, dwarfing deposit banking.

FATF has strongly recommended money laundering controls for the securities field since 1992, in conjunction with the Madrid-based International Organization of Securities Commissions (IOSCO), a global association of governmental bodies that includes the Commodity Futures Trading Commission (CFTC), which regulates the securities and futures markets. The difficulty in dealing with money laundering in the securities field is that typically little currency is involved. It is an industry that runs by electronic transfers and paper. Its use in the money laundering process is generally after launderers have placed their cash in the financial system through other methods.

Aspects of the securities industry that increase its exposure to money laundering include:

- International nature
- Speed of transactions
- Ability to conduct free-of-payment asset transfers, in which securities are transferred without a corresponding transfer of funds
- Ease of conversion of holdings to cash without significant loss of principal
- Routine use of wire transfers to, from, and through multiple jurisdictions
- Competitive, commission-driven environment, which, like private banking, provides ample incentive to disregard the customers' source of funds

- Practice of brokerage firms of maintaining securities accounts as nominees or trustees, thus permitting concealment of the identities of the true beneficiaries
- Weak AML programs that do not have effective CDD, suspicious activity monitoring, and other controls

The illicit money laundered through the securities sector can be generated by illegal activities, both from outside and within the sector. For illegal funds originating outside the sector, securities transactions for the creation of legal entities can be used to conceal or obscure the source of these funds (i.e., layering). In the case of illegal activities within the securities market itself (e.g., embezzlement, insider trading, securities fraud, and market manipulation), the transactions and manipulations generate illegal funds that must then be laundered. In both cases, the securities sector offers money launderers the potential for a double advantage: allowing them to launder illegal funds and acquire additional profit.

Money laundering can occur in the securities industry in customer accounts that are used only to hold funds and not for trading. This allows launderers to avoid banking channels for which the launderer believes there are more stringent money laundering controls. Other indications of money laundering are wash trading and offsetting transactions, which involve the entry of matching buys and sells in particular securities, creating the illusion of trading. Wash trading through multiple accounts generates offsetting profits and losses, as well as transfers of positions between accounts that do not appear to be commonly controlled.

The FATF *Money Laundering and Terrorist Financing in the Securities Sector* typologies report identifies the following areas as presenting the greatest money laundering vulnerabilities in the securities industry:

- Wholesale markets
- Unregulated funds
- Wealth management
- Investment funds
- Bearer securities
- Bills of exchange

Several compliance challenges that are unique to the securities sector include:

- **Variety and complexity of securities:** Security offerings are broad, with some products tailored to the needs of a single customer and others designed for sale to the general public. Products range from the simple and almost universally known to the relatively complex and esoteric. Some knowledge of the underlying security is typically required to address risk.
- **High-risk securities:** Although most securities are issued by legitimate companies, securities that are underregulated or established for illegitimate purposes pose risks. In the United States, securities that are not traded on regulated exchanges are typically sold over-the-counter, with tiers such as "pink sheets" that require only minimal reporting. These products make it easier to obscure information such as beneficial ownership and make it difficult to determine associations with sanctioned jurisdictions and companies. Securities firms are required to identify securities that might pose risks and develop processes to restrict trading of those securities, often on dozens of platforms.
- **Multiple layers and third-party risk:** The securities industry involves many participants, including financial organizations and broker-dealers, financial advisors, transfer agents, securities lenders, custodians, introducing brokers, and sales agents. The many layers of intermediaries, who may also cross borders, make standardizing controls difficult and further challenge overall compliance.

FATF has identified a number of suspicious indicators within the global securities markets. Those particularly relevant to the securities sector include:

- A customer with a significant history with the securities firm who abruptly liquidates all of her assets in order to remove wealth from the jurisdiction
- A customer who opens an account or purchases a product without regard to loss, commissions, or other costs associated with that account or product, including early cancellations of long-term securities
- A securities account that is used for payments or outgoing wires with little or no securities activity (e.g., account appears to be used as a depository account or a conduit for transfers)

- A customer's transactions that include a pattern of sustained losses, which might indicate the transfer of value from one party to another
- Transactions in which one party purchases securities at a high price and then sells them at a considerable loss to another party, which might indicate the transfer of value from one party to another
- A customer who is unfamiliar with a financial product's performance and specifications but wants to invest in it nonetheless
- A customer who is known to have friends or family who work for the securities issuer, or a trading pattern that suggests he might have nonpublic information
- Two or more unrelated accounts at a securities firm that trade an illiquid or low-priced security, or "penny stock," suddenly and simultaneously
- A customer who deposits physical securities that (1) are in large quantities; (2) are titled differently from the name of the account; (3) do not bear a restrictive legend, even though the history suggests that they should; or (4) lack sense in terms of the method by which they were acquired

Retail broker-dealers are the industry's frontline defense—and its most vulnerable access point. They are under constant management pressure to expand their client base and manage more assets. The more assets in a client's account, the more commission will be generated. Money launderers can potentially use this situation to their advantage by promising a large or steady commission stream. Therefore, it is important for broker-dealers to understand who they conduct business with and to monitor customers for suspicious activity.

In the United States, the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), as directed by the BSA's regulatory rules, implement requirements for broker-dealers at both small and large organizations. These requirements compel organizations to implement AML programs that include an appointed BSA officer, CDD, suspicious activity monitoring, training, and independent audits. They also subject broker-dealers to oversight by the SEC, FINRA, or both to monitor if and how they are complying with the AML program requirements. Weak or nonexistent AML program requirements can result in substantial monetary and criminal penalties.

Use of securities (Case example: Methods of money laundering)

In 2017, the Financial Conduct Authority (FCA) fined Deutsche Bank AG £163 million for the lack of an adequate anti-money laundering/countering the financing of terrorism (AML/CFT) control framework between 2012 and 2015.

During that time, Deutsche Bank failed to obtain sufficient information about its customers to inform the risk assessment process and ensure effective transaction monitoring. The infractions and resulting loopholes allowed the front office of Deutsche Bank's Russia-based subsidiary, DB Moscow, to execute more than 2,400 pairs of mirror trades between April 2012 and October 2014.

The FCA identified significant deficiencies in Deutsche Bank's AML control framework. Its Corporate Banking and Securities division (CB&S) in the UK had significant deficiencies, which contributed to the successful execution of the trades. The deficiencies included:

- Inadequate KYC and customer due diligence (CDD)
- Failure to ensure that the CB&S front office took responsibility for its KYC obligations
- Flawed customer and country risk-rating methodologies
- Deficient AML policies and procedures
- Inadequate AML information technology infrastructure
- Lack of automated AML systems for detecting suspicious trades
- Failure to provide adequate oversight of trades booked in the UK by traders in non-UK jurisdictions

The customers of the institutions in the UK and Russia used mirror trades to transfer more than US$6 billion from Russia. The funds went through Deutsche Bank in the UK to bank accounts located in Cyprus, Estonia, and Latvia. The orders for both sides of the mirror trades were received by DB Moscow, which executed both sides, or transactions, at the same time.

Investigators determined that the customers from Moscow and London who executed the mirror trades were connected to each other. In addition, the

volumes and values of the securities were the same on both sides. The customers were successful in changing rubles into US dollars and transferring those funds out of Russia. Deutsche Bank should have recognized these transactions as red flags for financial crime.

The inadequacy of Deutsche Bank's overall AML/CFT framework and governance made the fictitious mirror trades simple to execute. The importance of a robust AML/CFT framework and testing for reliability and effectiveness cannot be overemphasized.

Key takeaways

- Inadequate AML/CFT frameworks allow abuse of the financial system by criminals.
- Real-time mirror trades involve the rapid transfer of significant sums of money around the world.
- It is critical to have adequate KYC and CDD procedures in place to identify suspicious activity.
- Organizations need to undertake continuous risk assessment and ensure controls are in place to mitigate against existing, new, and emerging risks.

Securities and broker-dealers (Case example: Methods of money laundering)

In June 2020, Hong Kong's Securities and Futures Commission (SFC) fined Guotai Junan Securities (Hong Kong) Limited HK$25.2 million for multiple internal control failures and regulatory breaches of AML regulations, as well as its handling of third-party fund transfers, placing activities, and late reporting of wash trades. Wash trading is the illegal process of buying shares of a company through one broker, while selling shares through a different broker. Specifically, the SFC investigation found that, from 2014 to 2015, Guotai Junan failed to take reasonable steps to mitigate AML/CFT risks in relation to nearly 15,600 third-party deposits and withdrawals, totaling HK$37.5 billion.

The investigation determined that Guotai Junan did not respond to several red flags indicating that certain third-party fund transfers it processed were

suspicious. This resulted in a failure to monitor clients' activities, conduct proper scrutiny of the fund transfers, and report unusual and suspicious transactions to the local financial intelligence unit (FIU). More than 5,000 deposits were made by third parties into the dealer's client accounts without documenting the depositors' identities, their relationships with the account holders, and the purpose of the deposits. Similarly, when two deposits were made into a client account for the purpose of buying shares, the firm failed to recognize that the funding was coming from a third party.

Maintaining a solid understanding of one's customers and their business operations, scrutinizing their activity for any discrepancies, and performing KYC/CDD on any related and, particularly, unrelated third parties are key elements of an organization's AML/CFT program. Regulated entities are required to know the beneficial owners of their customers. It is also important to ascertain the source of wealth or funds in transactions. Guotai Junan failed to do so on several occasions, for example when HK$28.8 million used by five clients to purchase shares of a Hong Kong-listed company were deposited by the same third party in amounts that well exceeded their self-declared net worth.

Key takeaways

- Ongoing transaction monitoring is a key component of an effective AML/CFT compliance program.
- Share offerings have associated risks for money laundering, insider trading, and wash trades.
- Both potential and confirmed breaches should be promptly disclosed to the relevant regulator.

Nonfinancial Businesses and Professions

Casinos

Casinos are among the most proficient cash-generating businesses. High rollers, big profits, credit facilities, and a variety of other factors combine to generate a significant amount of cash that flows from the casino, or "house," to the players and back. Where gambling is legal, billions of dollars can readily flow between customers and a casino.

Casinos and other businesses associated with gambling, such as bookmaking, lotteries, and horse racing, are associated with money laundering because they provide an excuse for recently acquired wealth with no apparent legitimate source. The services offered by casinos vary, depending on the jurisdictions in which they are located and the measures taken in those jurisdictions to control money laundering.

Money laundering through casinos generally occurs in the placement and layering stage, for example, converting the funds to be laundered from cash to checks and using casino credit to add a layer of transactions before the funds are ultimately transferred out. A launderer can buy chips with cash generated from a crime and then request repayment by a check drawn on the casino's account. Often, rather than requesting repayment by check in the casino where the chips were purchased with cash, the gambler claims to be traveling to another country in which the casino chain has an establishment, requests credit to be made available there, and then withdraws it in the form of a check in the other jurisdiction. Money launderers can also establish casino lines of credit and use illegitimately obtained funds as a repayment on the credit lines.

FATF has reported that gaming businesses and lotteries are increasingly used by launderers. It gives examples of gambling transactions that enabled drug dealers to launder their money through casinos and other gambling establishments. One laundering technique connected with horse racing and gaming involves the person actually gambling the money to be laundered, but

in such a way that he is reasonably sure of ultimately recovering his stake in the form of checks issued or funds transferred by the gambling or betting agency and reflecting verifiable winnings. This method makes it more difficult to prove the money laundering, because the person has actually received proceeds from gambling.

Junkets, a form of casino-based tourism, also present significant money laundering risk, because junket participants largely rely on third parties, or junket operators, to move the funds across borders and through multiple casinos. This method creates layers of obscurity around the source of funds, ownership of the money, and the identities of the players. In some jurisdictions, casinos might enter into a contractual agreement with a junket operator to rent a private gaming room. In some situations, it is the junket operator, not the casino, that monitors player activity and issues and collects credit. Additionally, some jurisdictions allow junket operators to pool funds, which obscures the spending of individual customers. In certain regions, licensed junket operators act as fronts for junket operators in another country. The front operators supply players to a casino through the casino's licensed junket companies, which might not qualify for a license in the country where the players will be gambling. Such unlicensed sub-junket operators can act as credit collectors and might have ties to organized crime networks. This poses serious risk and can lead a casino to engage in informal arrangements with junket operators that are inconsistent with AML/CFT policies.

FATF recognizes that several jurisdictions do not require licensing of junket operators and their agents, further increasing the risks of money laundering. FATF emphasizes the need to ensure that junket operators are not under criminal influence and that financial transactions are transparent and subject to relevant AML/CFT measures.

FinCEN and FATF have identified specific behaviors to watch for, including:

- Attempts to evade AML reporting and recordkeeping requirements, such as:
    - A customer pays off a large credit debt, such as markers or bad checks, over a short period of time through a series of currency transactions, none of which exceeds the reportable threshold.
    - Two or more customers each purchase chips in small numbers, engage in minimal gaming, and then combine the funds to request a casino check for the chips presented.

- A customer receives a payout in excess of $10,000, but requests currency of less than $10,000 and the balance paid in chips. He then redeems the remaining chips in amounts lower than the reporting threshold.
- A customer structures a transaction, often by involving another customer, to avoid filing of a CTR or another tax form.
- When asked for identification, a customer reduces the number of chips presented for a cash-out to remain under the reportable threshold.

- Using the cashier's cage solely for its banking-like financial services, such as:
  - A customer wires funds derived from nongaming proceeds to or through a bank or nonbank financial organization located in a country that is not her residence or place of business.
  - A customer appears to use a casino as a temporary repository for funds by making frequent deposits into the casino account and, within a short period of time, requesting money transfers to a domestic or foreign-based bank account.
- Minimal gaming activity without a reasonable explanation, such as:
  - A customer purchases a large number of chips, engages in minimal gaming, and then redeems the chips for a casino check.
  - A customer uses an established casino credit line to purchase chips, engages in minimal gaming, pays off the credit in currency, and redeems the chips for a casino check.
  - A customer makes a large deposit using small-denomination bills, withdraws it in chips at the table, engages in minimal play, and then exchanges the chips at the cage for large-denomination bills.
  - A customer inserts a high number of small-denomination bills into a slot machine, known as “bill stuffing,” engages in minimal or no play, and exchanges the voucher for large-denomination bills or requests a casino check for what appears to be a legitimate winning credit from a slot machine.

- A customer frequently purchases chips with currency under a reportable threshold, engages in minimal play, and leaves the casino without cashing out the chips.
- A customer transfers funds to a casino for deposit into a front money account, withdraws it in chips at a table, engages in minimal play, and then asks for the chips to be exchanged for a casino check.

- Unusual gaming and transaction patterns, such as:
  - Two customers frequently bet large amounts to between them cover both sides of an even bet, such as betting both “red and black” or “odd and even” on roulette, betting both “with and against” the bank in baccarat and betting the “pass line” or “come line” and the “don’t pass line” and “don’t come line” in craps.
  - A customer routinely bets both sides of the same line for sporting events (i.e., betting both teams to win); the amount of overall loss to the customer is minimal, which is known as hedging.
  - A customer requests that a casino check be issued payable to third parties or without a specified payee.
  - A customer makes large deposits or pays off large markers with multiple instruments, such as cashier’s checks, money orders, traveler’s checks, and foreign drafts, in amounts of less than $3,000, indicating an attempt to avoid identification requirements.
  - A customer withdraws a large amount of funds from a deposit account and requests that multiple casino checks be issued, each less than $10,000.
  - A customer establishes a high-value deposit that remains dormant for an extended period of time and then withdraws or transfers the funds.

The risk of money laundering arises not only from specific customer behaviors, but also from the types of customers casinos conduct business with. A player often builds a reputation as a high roller as long as they show big play, without being subject to the due diligence necessary to determine the source of funds. It is a serious mistake for casinos to allow play and accept the revenue without reasonably determining the source of a customer’s gaming funds. FinCEN expects US casinos to know the source of high rollers’ funds. Even when they are not explicitly required to determine the source of funds, it

is recommended that casinos require more information from certain customers who engage in high-risk transactions, such as international wire transfers and large cash deposits, as part of a risk-based approach to AML/CFT.

Through FinCEN, the US has become one of the most aggressive authorities on issuing AML program deficiency penalties to some of the largest casinos in the industry, for example:

- **Tinian Dynasty Hotel & Casino fined US$75 million (2015):** The casino failed to develop and implement an AML program (i.e., no dedicated AML officer, failure to develop and implement AML policies and procedures, and no independent tests of the AML program). The casino failed to file thousands of CTRs, and its employees assisted wealthy VIP patrons in completing suspicious transactions, particularly structuring.
- **Caesars Palace fined US$9.5 million (2015):** The casino "allowed some of the most lucrative and riskiest financial transactions to go unreported"; promoted private salons in the United States and abroad without appropriately monitoring transactions, such as wire transfers, for suspicious activity; and openly allowed patrons to gamble anonymously.
- **Sparks Nugget fined US$1 million (2016):** The casino "had a systemic breakdown in its compliance program" and disregarded its compliance manager. Rather than file proper SARs, Sparks Nugget instructed the compliance manager to avoid interacting with regulatory auditors and prevented her from reviewing a copy of the completed regulatory exam report.
- **Artichoke Joe's Casino (AJC) fined US$8million (2017):** AJC senior managers were aware that loan sharks were conducting criminal activity through the card club and using AJC gaming chips for money laundering. They nonetheless failed to file any SARs, although on multiple occasions loan sharks had provided AJC chips to customers on the gaming floor in plain sight. AJC also failed to implement adequate internal controls.

In addition to ensuring adequate recordkeeping and reporting requirements, casino AML/CFT programs should establish a process that enables the casino to reasonably determine sources of funds and allows CDD to be conducted at the time the funds are accepted, often with a customer already on the

property and ready to game, rather than relying exclusively on an after-the-fact back-of-house compliance investigation.

Although the concept of on-demand enhanced KYC and source of fund questioning might be new to casinos, there are many ready-to-use tools developed specifically for the industry's front-of-house operations. The most effective processes combine information from various international sources—criminal and judicial, securities and exchanges, financial, government and worldwide lists, political exposure, negative news, and business associations—with ID verification, making the due diligence possible directly from the front line of operations.

Online casinos and gaming operations are increasingly prevalent. Online gaming is regulated in certain jurisdictions; however, many online gaming companies operate illegally. In the United Kingdom, the Gambling Commission requires a license for remote gambling when the business operates in the UK and any part of its gambling equipment is located in the UK, and when the equipment is located outside the UK, but the business operates through a British-facing business. Online gaming is also regulated in Antigua and Barbuda under the Interactive Gaming and Interactive Wagering Regulations, and companies are required to establish compliance programs.

Nevertheless, online gambling provides an effective method of money laundering for cybercriminals, because transactions are conducted principally through credit and debit cards. Site operators are typically unregulated offshore organizations. This can affect financial organizations, because the internet gambling sites often have accounts in offshore banks that, in turn, use reputable domestic correspondent banks. Tracing the source and ownership of illegal money that moves through these accounts can be difficult for enforcement and regulatory agencies.

Due to the inconsistent regulatory environment and susceptibility to cybercriminals, some credit card issuers do not allow the use of their credit cards for online gambling. Financial organizations screen merchant codes that identify the type of business accepting the credit card and transaction codes for "card not present" (i.e., the cardholder is not physically in the casino to process the transaction via a card reader). The bank can thus block internet gambling transactions. However, online gambling can be funded in numerous ways other than credit cards, such as prepaid cards, wire transfers, peer-to-peer transfer, virtual currency, and mobile phone carrier billing.

MONEYVAL, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, identified numerous potential typologies and red flag indicators for money laundering involving online gambling, including the following examples:

- A money launderer colludes with an operator of an offshore online gambling operation and deposits funds obtained from criminal activities into the gambling account and then withdraws them as winnings. The website operator keeps a percentage of the proceeds as a commission. The launderer declares the winnings to the tax authorities and then uses the funds for legitimate purposes.
- A money launderer deposits funds into an online gambling account using a stolen identity. He bets using the funds and receives payouts for the winnings or sustains acceptable losses.
- A money launderer logs on to the gambling account from multiple countries.
- A player is identified as a PEP.

Casinos (Case example: Methods of money laundering)

In 2019, the Australian Independent Liquor & Gaming Authority (ILGA) launched an inquiry into the operations of Crown Melbourne, an Australian land-based casino operator. ILGA alleged that Crown had actively facilitated money laundering on behalf of extremely wealthy Chinese gamblers since 2014.

The inquiry highlighted the systemic failures of key AML controls such as accepting large cash deposits from Chinese nationals at cashier's desks in a VIP room operated by a junket agency. Crown also incorporated shell companies to facilitate transactions from China that were not reported to the regulator, the Australian Transaction Reports and Analysis Centre.

Whistleblowers leaked video of a cashier's desk where a VIP customer exchanged bricks of loose cash, totaling hundreds of thousands of AUD, for high-value chips. Whistleblowers claimed similar transactions occurred

regularly in Crown's VIP rooms, one of which was operated independently by junket agents that recruited high-rolling gamblers from Macau.

Crown used two shell corporations to enable VIP gamblers and junket agents to circumvent Chinese capital flight controls to credit casino accounts and settle gambling debts. There was evidence that international criminal gangs exploited these accounts to place proceeds of crime.

Crown staff often aggregated multiple deposits in one entry to hide from the AML team the number and nature of transactions. Evidence of structuring included nearly 700 deposits made below reporting thresholds, often the same individual making multiple deposits at multiple branches on the same day. Customers were allowed to deposit cash at Commonwealth Bank of Australia without verifying identity or source of funds. Crown repeatedly failed to report transactions exceeding the AUD physical currency reporting threshold.

Key takeaways

- Casino cashiers can be exploited for placement.
- Intermediaries, such as junket agents and shell companies, can be used to place, layer, and integrate funds through casino operations.
- A VIP customer's commercial value must not protect them from suspicion, scrutiny, or AML controls.

Dealers in High-Value Items (Precious Metals, Jewelry, Art, etc.)

The European Directives on money laundering provide a common framework for including trade in precious metals, such as gold and diamonds, and other high-value items, such as jewelry and art, within AML monitoring programs. The USA PATRIOT Act requires certain dealers in covered and finished goods, including precious metals, stones, and jewels, to establish AML programs. However, in many other jurisdictions, these industries are not regulated for money laundering control purposes.

FATF released a report entitled *Money Laundering/Terrorist Financing Risks and Vulnerabilities Associated with Gold*, which reinforced prior typology

reports. Gold has high intrinsic value in a relatively compact form that is easy to transport. It can be bought and sold simply and often anonymously for currency in most areas of the world. It is more readily accepted than precious stones, especially because it can be melted down into many different forms. Gold holds its value regardless of the form it takes—whether as bullion or as a finished piece of jewelry—and is thus often used to facilitate the transfer of wealth. For some societies, gold carries an important cultural or religious significance that adds to its demand.

Following are two of the key findings from the report:

1. Gold is an extremely attractive vehicle for laundering money. It provides a way for criminals to convert their illicit cash into anonymous transferable assets.
2. The gold market is a target for criminal activity because it is lucrative. Understanding and knowing the various stages of the gold market and types of predicate offenses is critical in identifying money laundering.

In industries that deal in high-value items, it is possible that transactions in a particular scheme have not taken place at all, but they are represented with false invoicing. The paperwork is then used to justify transferring funds to pay for the shipments. The false invoicing scheme, whether overbilling or underbilling for the reputed goods or services provided, is a common money laundering technique.

The following transactions are also vulnerable and require additional attention:

- **Payments or returns to persons other than the owner:** A transaction is suspicious if one person delivers precious metal for refining and asserts ownership of the metal and authority to sell it, but directs payments to be made to another person. It is possible that the "dealer in precious metal" is being used to transfer an asset not only from one form into another—unrefined gold to refined gold or money within the international finance system—but also from one person to another.
- **Precious metal pool accounts:** These accounts are maintained by a small number of large and sophisticated precious metal companies and have worldwide scope. They receive and hold precious metal credits for a customer, which can be drawn on by that customer. The customer can request the return of the precious metals, the sale and return of monetary proceeds, or the delivery of precious metal to another person. Thus, a

refining customer in one country can deliver gold scrap for refining, establish a gold credit in the refiner's pool account system, and subsequently have delivery made by the refiner to another person, based upon that credit.

The illegal trade of diamonds is an important factor in armed conflicts in certain areas of the world, and terrorist groups can use diamonds from these regions to finance their activities.

Individuals and entities in the diamond sector have also been involved in complex diamond-related money laundering cases. As with gold, the simplest typology involving diamonds consists of the direct purchase of the gems with illegally obtained money.

Regarding dealers in high-value items, FATF reports that common types of laundering activities include retail foreign exchange transactions, forged or fraudulent invoicing, commingling of legitimate and illicit proceeds in the accounts of diamond trading companies, and, in particular, international fund transfers among these accounts. Some of the detected schemes are covers for laundering the proceeds of illicit diamond trafficking. In others, diamond trading is used as a method for laundering the proceeds of other criminal activity.

The multi-million-dollar fine art industry can also serve as a convenient money laundering vehicle. Anonymous agents at art auction houses bid millions of dollars for priceless works. Payment is later wired to the auction house by the agents' principals from accounts in offshore havens. It is a convenient mechanism for money launderers.

Art and antiques dealers and auctioneers can follow these tips to decrease their money laundering risks:

- Require all art vendors to provide their names and addresses. Require them to sign and date a form that states that the item was not stolen and that they are authorized to sell it.
- Verify the identities and addresses of new vendors and customers. Be suspicious of any item with an asking price that does not reflect its market value.
- If there is reason to believe that an item was stolen, immediately contact the Art Loss Register, the world's largest private database of stolen art, antiques, and collectibles. The database contains more than 700,000 items

reported by law enforcement agencies, insurers, and individuals as being stolen.

- Critically assess the situation when a customer asks to pay in cash. Avoid accepting cash payments unless there is a strong and reputable reason.
- Be aware of money laundering regulations.
- Appoint a senior staff member to whom employees can report suspicious activities.

Use of precious metals and gems to launder money (Case example: Methods of money laundering)

Operation Apex was a US multiagency operation that in 2020 targeted two US businesses and led to the arrest of 12 people. Individuals in the US, Hong Kong SAR, Mexico, Canada, and elsewhere were alleged to be members of the Wu gang, a transnational criminal organization engaged in wildlife trafficking, shark finning, drug trafficking, and money laundering using gold, precious metals, and diamonds.

The Wu gang allegedly trafficked marijuana grown in California to other parts of the US and ran two companies involved in the illegal wildlife trade, particularly shark finning.

Shark finning is legal in the US state of Florida, but not legal in the US state of California. The Wu gang used false documentation to establish and use a Florida shark fin business as a front for their California business, which shipped fins to Hong Kong. Fake invoices and paperwork were created to make it appear as though the Florida company was invoicing and financing the shark fin business.

Couriers were paid shipping fees to take bundles of cash to be laundered. The proceeds from the shark finning and drug trafficking were deposited into third-party business accounts that dealt in gold, precious metals, and jewels to hide the illegal activities. The accounts were held in financial organizations located in the United States, Mexico, and Hong Kong SAR. Criminals often use precious metals and gems to launder money because they make it easy to transfer value across borders, they have high value in a compact form, they

hold value over time, they are easily transported, their origins are difficult to trace, and they are easily exchanged for cash or used as currency.

Authorities confiscated US$4 million from the bank accounts of the two US businesses, $US1 million in diamonds, and approximately US$3 million in gold, silver, and other precious metals. They also seized about 18,000 marijuana plants, 34.5 pounds of processed marijuana, multiple guns, and more than six tons of shark fins.

Key takeaways

Converting illicit proceeds into precious metals and gems is attractive to financial criminals because:

- They have high value in a compact form, and their value tends to hold for long periods of time.
- They are easy to transport, so value can be transferred across borders without customs declarations.
- Their origins are difficult to trace.
- They can be easily exchanged for cash or used as currency in most areas of the world.

Use of precious metals to conceal drug proceeds (Case example: Methods of money laundering)

In 2018, a US gold refinery, Elemetal LLC, pled guilty to a charge of failing to maintain an adequate AML compliance program, despite refining billions of dollars' worth of gold from multiple countries. Elemetal had a designated compliance officer and an AML policy, but it failed to focus its associated activities on the specific risks of the precious metals industry. Due to its inadequate compliance program, Elemetal did not undertake basic KYC, customer due diligence (CDD), or enhanced due diligence (EDD) measures on its counterparties or establish the origin of the gold.

Elemetal forfeited US$15 million; was subjected to a five-year probation period, during which it was banned from acquiring gold from outside of the US; and agreed to implement a court-approved compliance and ethics program.

In 2015, the Financial Action Task Force (FATF) highlighted the AML risks inherent in the gold trade, due to its heavy reliance on cash as a method of exchange, the anonymity of the properties of gold making, and the extreme difficulty of tracing the origins of gold. US federal law requires precious metal dealers to maintain AML programs, recognizing the high risks of money laundering associated with gold.

In 2018, Elemetal admitted that it had failed to implement an adequate AML compliance program, leading to significant KYC, CDD, and EDD failures. Elemetal had acquired gold from overseas suppliers, including those in Central America, South America, and the Caribbean. However, it had not obtained confirmation of the suppliers' identities or the source and origin of the gold, in contravention of the KYC requirements of the Bank Secrecy Act (BSA). Elemetal sourced gold from suppliers for which AML screening would likely have flagged suspicious activity. It also accepted gold from countries and customers where records indicated the gold was likely being smuggled across borders. Elemetal accepted gold from suppliers for whom criminality was suspected due to negative press indicating they were trading in illicit gold.

Three former employees also pled guilty to importing illicit gold from South America into the US. These employees smuggled the illicit gold through an Elemetal subsidiary in Miami, falsified paperwork, and bribed South American officials. The three received prison sentences ranging from six to seven and a half years.

Following the court case, Elemetal was removed from the London Bullion Market Association’s list of gold refiners, from which buyers typically select their suppliers. COMEX, the largest gold futures market in the world, also refused to take gold from Elemetal.

Key takeaways

- US federal law requires precious metal dealers to maintain robust AML programs.
- AML risks inherent in the gold trade include heavy reliance on cash, anonymity, and difficulty tracing the source and origin of gold.

- The BSA requires precious metals dealers to perform KYC on suppliers and identify the source and origin of metals.
- In addition to KYC, AML programs must also implement Know Your Employee controls.
- Failure to implement robust AML controls can lead to significant fines, loss of business, and reputational damage.

Use of art to launder money (Case example: Methods of money laundering)

For several reasons, criminals consider the world of fine art and antiquities an attractive avenue for money laundering. It is a market that often operates with anonymity, such as private sales with third parties. It involves high-value goods with prices that are open to manipulation and subjectivity, and funding sources can be opaque. The art world also is spread throughout multiple international markets and commonly uses intermediaries and offshore accounts. Historically, a lack of regulation and supervision has been used to legitimize criminal activity in this market.

However, as increased regulation has made traditional methods of money laundering more difficult, the art world has attracted money launderers. There have been relatively few criminal convictions for money laundering in art and antiquities, but there have been several high-profile trials for theft and fraud in these markets. The art market has attracted the attention of regulators, and global authorities have enacted laws to prevent its misuse by organized criminals and terrorists.

In 2016, US biodiesel businessman Philip Rivkin pled guilty in Houston, Texas, to laundering US$78 million through many avenues, including purchasing over 2,000 pieces of art. He was sentenced to 10 years imprisonment and fined US$138 million in restitution and forfeiture. Investigators determined that Rivkin's company Green Diesel was not in fact producing biodiesel, but merely selling certificates and defrauding its customers. Rivkin sold falsified energy credits to large companies. With the proceeds, he bought a collection of photography worth over US$15 million, using the art to legitimize his income.

The Panama Papers scandal—the 2016 leak of millions of files from an offshore law firm—suggested connections between art and money laundering by

identifying suspicious shell companies that were investing in high-value art. A 2020 US Senate investigation determined that, within months of the US imposing sanctions on the Russian brothers Arkady and Boris Rotenberg, they illegally spent more than US$18 million on art in the US using shell companies linked to Russian oligarchs to evade sanctions.

The US, through the Anti-Money Laundering Act of 2020, has designated art markets as high-risk environments for money laundering and terrorist financing, as have the UK and the EU. These countries have promoted prevention through enhanced supervision and regulatory requirements. The EU, in response to the Fifth Directive regarding money laundering, released the Responsible Art Market Initiative, a set of guidelines on combatting money laundering and terrorist financing in the art market. As of January 2020, the Directive puts art market participants in the same category as financial institutions and estate agents. They now must register with regulators, perform due diligence on buyers and sellers, and take a risk-based approach to prevent money laundering.

Art dealers and associated financial services must understand money laundering methods and recognize red flags and the potential risks to their businesses. Many have invested in technology to assist with performing CDD, verification, and appropriate risk assessments. Still, the responsibility for due diligence remains with the art market participants.

Key takeaways

- Art markets are high risk. They are linked to serious criminal and terrorist offenses, due to the perceived anonymity of transactions, high value, and international movement of goods.
- Shell companies are often used to enhance secrecy.

- Governments have introduced primary and secondary legislation to regulate and enforce money laundering and terrorist financing standards across the art markets, including the following:
    - The Responsible Art Market Initiative
    - The Anti-Money Laundering Act of 2020
    - The EU Fifth Directive
- Art market participants are expected to understand the anti-money laundering requirements and are personally liable for noncompliance.

Travel Agencies and Websites

Travel agencies and their websites can also be used by money launderers to mix illegal funds with clean money to make the illegal funds appear legitimate, by providing a reason to purchase high-priced airline tickets, hotels, and other vacation expenses.

Money laundering can occur in travel agencies and through their websites in the following ways:

- Purchasing an expensive airline ticket for another person who then asks for a refund
- Paying for services in installments that are actually structured wire transfers in amounts small enough to avoid recordkeeping requirements, a method used especially by criminals from foreign countries
- Establishing tour operator networks with false bookings and documentation to justify significant payments from foreign travel groups

Travel agencies (Case example: Methods of money laundering)

In 2015, Indonesian militant suspect Gigih Rahmat Dewe opened a travel agency on Bintan Island, Indonesia, as a cover for the terrorist organization the Islamic State of Iraq and Syria (ISIS). The agency was initially funded by

US$2,800 provided by Dewe's handler, Bahrun Naim, an ISIS operative in Syria who was known to have been involved in several terrorist plots in Indonesia.

The travel agency's mission was to facilitate the safe travel of terrorists to their assignments, provide a legitimate cover for money laundering, and generate revenue to fund terrorist attacks. The plan only worked for a few months before the Indonesian National Police's counter-terrorism squad arrested Dewe and his accomplices for planning an attack on the Marina Bay Sands, a luxury hotel in Singapore.

Small travel agencies, especially in developing countries, are cash-intensive businesses that offer the same opportunities as other cash-intensive businesses to money launderers and terrorists. They also offer opportunities for terrorists to address logistical challenges, such as planning travel for terrorists and entering false identities into travel arrangements, all while limiting the risk of detection. ISIS created the travel agency in Indonesia to facilitate safe travel for terrorists and avoid detection.

As cash-intensive businesses, travel agencies also provide the ability to commingle legitimate and illegitimate funds and therefore launder money. This method can be used during all three stages of money laundering, because travel arrangements can be paid for in cash or by third parties and later refunded by known airlines or hotel chains in wire transfers. This transfer of funds would raise minimal suspicion at recipient banks. Payments are overseen by the criminals controlling the travel agency, so the cash and third-party payments can be hidden.

Key takeaways

- Travel agencies are cash-intensive businesses.
- Travel agencies solve logistics problems for terrorists.
- Travel agencies can allow the use of false identities.
- Travel agencies can be used to commingle legitimate and illegitimate fund.
- Travel agencies can be used in all three stages of money laundering.

Vehicle Sales

The vehicle sales industry includes sellers and brokers of new vehicles, such as automobiles, trucks, and motorcycles; new aircraft, including fixed-wing airplanes and helicopters; new boats and ships; and used vehicles.

Money laundering risks, methods, and red flags in the vehicle sales industry include:

- Structuring cash deposits below the reporting threshold
- Purchasing vehicles with sequentially numbered checks or money orders
- Trading in vehicles and conducting successive transactions of buying and selling new and used vehicles to produce complex layers of transactions
- Accepting third-party payments, particularly from jurisdictions with ineffective money laundering controls

Most money laundering cases involving vehicle dealers have one common element: the unreported use of currency to pay for the automobiles.

Cases have also occurred in which car dealers laundered money by allowing drug dealers to trade in cars for less expensive models and to be paid in checks, not cash, for the difference. In one such down-trading money laundering scheme, a drug dealer traded in his US$37,000 Porsche for a US$17,000 Ford Bronco. The car dealer allowed the down-trade, knowing that the customer was a drug dealer, in violation of the anti-money laundering law.

Luxury vehicles (Case example: Methods of money laundering)

In May 2019, a US federal court sentenced John D. Leontaritis, a resident of Texas, to 20 years in federal prison. He was convicted of drug trafficking and money laundering violations that were committed from 2013 to 2017 in Texas. A jury had found Leontaritis guilty of conspiracy to possess drugs with the intent to distribute, the distribution of methamphetamine, and conspiracy to commit money laundering. The latter offense included using his luxury car dealership to launder the proceeds of drug sales for the benefit of a sprawling interstate drug trafficking network.

Leontaritis was the owner and operator of Vanderhall Exotics of Houston LLC, which specialized in exotic luxury automobiles. He used his car dealership to launder drug money for a large Houston-based drug trafficking organization that smuggled drugs from Mexico into the US.

Leontaritis knowingly laundered drug profits through his business by regularly accepting cash payments from known drug dealers in exchange for high-value vehicles. As part of the conspiracy, Leontaritis used fraudulent dealer invoices to hide the true identities of the buyers from law enforcement and the Internal Revenue Service and failed to report cash payments for vehicles. The conspiracy operated for many years and involved hundreds of kilograms of Mexican-origin methamphetamine. Leontaritis laundered millions of dollars through the dealership before his criminal enterprise was dismantled by the US Organized Crime Drug Enforcement Task Force.

Key takeaways

- Cash-intensive businesses, such as car dealerships, are particularly vulnerable to money laundering.
- Fraudulent invoices can be used to hide buyers' identities.
- The purchase of luxury vehicles and other assets can be used to place large amounts of illicit money into the financial system seemingly legitimately.

Gatekeepers: Notaries, Accountants, Auditors, and Lawyers

Many professionals have the ability to either block or facilitate the entry of illegitimate money into the financial system, including lawyers, accountants, company formation agents, auditors, and other financial intermediaries.

The responsibilities of such gatekeepers include identifying clients, conducting due diligence on their clients, maintaining records about their clients, and reporting suspicious client activities. Some of these obligations also prohibit gatekeepers from informing, or "tipping off," clients who are the subject of SARs. Violations can subject gatekeepers to prosecution, fines, and even imprisonment.

In European Union countries and several others, mandatory anti-money laundering duties apply to gatekeepers. FATF's 40 Recommendations (see the chapter "Anti-Money Laundering/Countering the Financing of Terrorism Compliance Programs" for more on the Recommendations) also cover independent lawyers, legal professionals, and other gatekeepers.

FATF identified the following functions provided by lawyers, notaries, accountants, and other professionals as the most useful to potential money launderers:

- Creating and managing corporate vehicles and other complex legal arrangements, such as trusts, which might obscure the links between the proceeds of a crime and the perpetrator
- Buying or selling property: Property transfers can serve as the cover for illegal fund transfers (layering stage) or the final investment of proceeds after they pass through the initial laundering process (integration stage).
- Performing financial transactions: These professionals might carry out various financial operations on behalf of a client (e.g., issuing and cashing checks, making deposits, withdrawing funds from accounts, engaging in retail foreign exchange operations, buying and selling stock, and sending and receiving international funds transfers).
- Providing financial and tax advice: Criminals with large amounts of money to invest might pose as legitimate businesspeople to minimize tax liabilities or place assets out of reach in order to avoid future liabilities.
- Providing introductions to financial organizations
- Undertaking certain litigation
- Setting up and managing charities

Criminals often use legal professionals to give the appearance of respectability in order to dissuade questioning or suspicion from financial organizations and to create an added step in the chain of any possible investigations. Additionally, legal professionals might deliberately misuse a client's legitimate accounts to conduct transactions without the client's knowledge.

The FATF report also describes five categories of red flag indicators of money laundering or terrorism financing:

1. Characteristics of the client:
    - Overly secretive
    - Uses an agent or an intermediary or avoids personal contact without a logical reason
    - Reluctant to provide or refuses to provide information or documents usually required to enable the execution of a transaction
    - Holds or has previously held a senior public position or has professional or family ties to such individuals
    - Known to have been the subject of investigation for an acquisitive crime (i.e., one in which the offender derives material gain from the crime, such as theft or embezzlement)
    - Known to have ties to criminals
    - Shows unusual interest and asks repeated questions on the procedures for applying ordinary standards
2. Characteristics of the involved parties:
    - Native to, residents in, or incorporated in a high-risk country
    - Connected without an apparent business reason; that is, tied in a way that generates doubts as to the real nature of the transaction
    - Appear in multiple transactions over a short period of time
    - Incapacitated or under legal age, with no logical explanation for their involvement
    - Attempt to disguise the real owner or parties to the transaction
    - Not directing the transaction, (i.e., the person directing the operation is not one of the formal parties to the transaction)
    - Do not appear to be suitable representatives
3. Characteristics of the source of funds:
    - Provided using unusual payment arrangements
    - Collateral located in a high-risk jurisdiction
    - Represents a significant increase in capital for a recently incorporated company, including foreign capital, without a logical explanation

- Represents unusually high capital in comparison with similar businesses
- Stems from a security transferred with an excessively high or low price attached
- Stems from large financial transactions that cannot be justified by the corporate purpose

4. Characteristics of the lawyer:
    - Located at a significant distance from the client or transaction without a legitimate or economic reason
    - Little or no experience in providing the specific services needed
    - Being paid substantially higher than usual fees without a legitimate reason
    - Frequently changed by the client, or the client has multiple legal advisors without legitimate reason
    - Provides services previous refused by another professional
5. Characteristics of the retainer:
    - Transactions that are unusual with regard to the type of operation and the transaction's typical size, frequency, or execution
    - Transactions that do not correspond to the client's normal business activities and show that he does not have a suitable knowledge of the nature, object, or purpose of the professional performance requested
    - Creation of complicated ownership structures or structures with involvement of multiple jurisdictions without a legitimate or economic reason
    - Client transaction history with no documentation to support company activities
    - Inconsistencies and unexplained last-minute changes to instructions
    - No sensible commercial, financial, or tax reason for the transactions or increased complexity that unnecessarily results in higher taxes or fees
    - Exclusively keeping documents or other goods, or holding large deposits or otherwise using the client account without provision of legal services

- Abandoned transactions without concern for fee level or after the receipt of funds
- Power of attorney sought for the administration or disposal of assets under unusual circumstances without logical reason
- Litigation that is settled too easily or quickly with little or no involvement of legal professional retained
- Requests for payments to third parties without substantiating reason or corresponding transaction

The issue of requiring attorneys to be gatekeepers in the AML/CFT area can be controversial, given the fact that attorneys have confidential relationships with their clients. Various alternatives have been discussed and debated, including:

- Deferring regulation until adequate education is conducted
- Imposing internal controls and due diligence duties on lawyers regarding unprivileged communications
- Using a joint government-private sector body to regulate lawyers who engage in financial activities, requiring registration with and regulation by an agency
- Devising a new hybrid approach, such as through guidance notes and best practices standards from FATF

Gatekeeper issues in the United States are focused on the scope of the requirements, particularly the definition of the financial transactions to which reporting requirements apply. Many regulators within the United States want the scope to coincide with the European Union Directive, which requires EU members to ensure that obligations are imposed on a wide range of professionals, including auditors, attorneys, tax advisors, real estate agents, and notaries.

The extraterritorial reach of several existing US initiatives subject lawyers who conduct international transactions to various requirements.

Gatekeepers (Case example: Role of gatekeepers in facilitating money laundering)

The Organisation for Economic Co-operation and Development (OECD) publication, *Ending the Shell Game: Cracking Down on the Professionals Who Enable Tax and White-Collar Crimes*, highlights that, "White collar crimes like tax evasion, bribery, and corruption are often concealed through complex legal structures and financial transactions facilitated by lawyers, accountants, financial institutions and other 'professional enablers' of such crimes." The report was issued to ensure that professional service providers are aware of their responsibilities to identify, report, and avoid money laundering risks and to provide strategies for countries to take action against criminals who abuse their positions to conceal and facilitate illegal activity.

In January 2019, UK lawyer Ross McKay was sentenced to prison for seven years, stripped of his license to practice, and required to pay £1,450 in costs for helping organized criminals launder money via mortgage fraud.

McKay also suffered personal consequences. He damaged his reputation, lost his livelihood, and left a wife and three young children with no financial support for the time he was in prison.

The majority of professional service providers in gatekeeping positions, such as lawyers, accountants, and financiers, play an important role in the financial system and offer valuable legitimate services. However, because these professionals provide a veneer of respectability and offer a level of knowledge and skill that criminals might not possess, they are often engaged and employed by criminals to facilitate their illegal activities. In fact, a criminal organization's business typically mirrors that found in a legitimate environment. Some gatekeepers unwittingly assist in this illegal activity. However, in some cases, they are complicit in facilitating and concealing their clients' criminal activities.

McKay was a "go-to," or preferred, lawyer for criminals because he did not conduct basic KYC checks, including understanding the nature of the client's business, inquiring about the source of funds, or understanding connections between the parties and transactions.

McKay conducted more than 80 criminal transactions that helped a buy-to-lease landlord use illicit money to fraudulently build a £10.8 million property empire. McKay committed mortgage fraud by disguising the source of funds for property deposits and used nominee names instead of the names of the legitimate purchasers on mortgage applications. McKay also was the in-house lawyer for a loan company that was a front to launder criminal proceeds. The company belonged to a crime lord who was convicted of drug dealing.

McKay admitted that he knew the property transactions were being made to launder money and that he was deliberately dishonest in facilitating them.

Key takeaways

- Lawyers, accountants, financiers, and other "professional enablers" can abuse their positions to facilitate financial crimes via seemingly legitimate means.
- Professional service providers need to be aware of their responsibilities to identify, report, and avoid money laundering risks.
- Professional service providers need to ensure that they understand all the laws and regulations that apply to them, particularly when involved in multijurisdictional business.
- Professional enablers who commit crimes can be imprisoned and will likely be unable to operate again within their chosen profession.

Role of Gatekeepers (Case example: Special skills)

An attorney was convicted by a jury of conspiracy to commit money laundering. The attorney had helped to invest his client's drug proceeds by forming a corporation in the name of the client's wife and arranging a loan from the corporation to another (noncriminal) client. He then drafted a fake construction work contract, making the repayment of the loan appear to be payment for construction work performed by the company. He also drew up a promissory note, which the wife signed, but he did not provide copies of the note to either party. The attorney also advised his client how to deposit the cash from the loan without triggering reporting requirements. The appeals

court upheld the attorney's conviction but remanded him for resentencing after finding that the district court abused its discretion by not applying a sentencing enhancement based on the attorney's use of special skills (i.e., legal skills) in committing the offenses of conviction.

Key takeaways

- Gatekeepers can help disguise the source of illicit funds so they appear to originate from a legitimate business activity, such as a sale or loan.
- Money laundering schemes facilitated by gatekeepers can involve multiple parties, some of whom might not be aware of their own involvement.
- The special skills of gatekeepers enable them to help their clients evade detection using sophisticated money laundering schemes.

Investment and Commodity Advisors

Commodity futures and options accounts are vehicles that could be used to launder illicit funds. What are they?

- **Commodities:** Goods such as food, grains, and metals that are usually traded in large amounts on a commodities exchange, typically through futures contracts
- **Futures/futures contracts:** Contracts to buy or sell a set quantity of a commodity at a future date at a set price
- **Options/options contracts:** Contracts that create the right, but not the obligation, to buy or sell a set quantity of something, such as a share or commodity, at a set price after a set expiration date
- **Commodity pool:** A combination of funds from various investors to trade in futures or options contracts
- **Omnibus accounts:** Accounts held by one futures commission merchant (FCM) for another, in which case transactions of multiple account holders are combined, and their identities are unknown to the holding FCM

Commodity trading advisors (CTAs) engage in the business of advising others, either directly or indirectly, regarding the value or advisability of trading

futures contracts, commodity options, and swaps. They issue analyses and other reports concerning trading futures and commodity options and are also responsible for trading managed futures accounts. By directing such accounts, CTAs are in a unique position to observe activity that might suggest money laundering. As such, they need to be aware of what types of activities indicate potential laundering and terrorist financing and should implement compliance programs to detect and deter such activities.

Other professionals with similar responsibilities include:

- **Commodity pool operator:** Operator or solicitor of funds for a commodity pool, which combines funds from members and trades futures or options contracts
- **Futures commission merchant (FCM):** A firm or person that solicits or accepts orders on futures contracts or commodity options and accepts funds for their execution
- **Introducing broker-dealer in commodities (IB-C):** A firm or person that solicits and accepts orders for commodity futures from customers but does not accept funds. IB-Cs can be guaranteed or independent:
    - **Guaranteed introducing broker-dealer:** An IB-C with an exclusive written agreement with a futures commission merchant, which obligates the FCM to assume responsibility for the IB-C's performance
    - **Independent introducing broker-dealer:** An IB-C who is subject to minimum capital and financial reporting requirements, and who may introduce accounts to any FCM
- **Investment advisor:** Provides advice on securities and investments and manages client assets

The investment and commodity advising industry is susceptible to money laundering in the following ways:

- Withdrawal of assets through transfers to unrelated accounts or high-risk jurisdictions
- Frequent additions to or withdrawals from accounts
- Clients invest via checks drawn on, or wire transfers from, accounts of third parties with no relation to them

- Clients request custodial arrangements that allow them to remain anonymous
- Transfers of funds to the investment advisor, followed by transfers to accounts at other institutions that suggest a layering scheme
- CTAs or other professionals invest illegal proceeds for a client
- Movement of funds to disguise their origin

Trust and Company Service Providers

Trust and company service providers (TCSPs) are gatekeepers who set up trusts between parties and provide certain legal and administrative functions for corporations. According to the FATF report Guidance for a Risk-Based Approach for Trust and Company Service Providers, TCSPs include any person or business that provides any of the following services to third parties:

- Acting as an agent on behalf of legal persons to form a company
- 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 correspondence for a company, partnership, or any other legal person or arrangement
- Acting as (or arranging for another person to act as) a trustee of an express trust
- Acting as (or arranging for another person to act as) a nominee shareholder for another person

The FATF report emphasizes the need for TCSPs to obtain detailed information on customers and the need for them to understand the source of funds and the general purpose of the structures they create for their clients' benefit. In addition, TCSPs should always be able to identify the beneficial owners and controlling persons for an account.

The FATF report also points out that some jurisdictions regulate TCSPs like lawyers, meaning that clients can request confidentiality, thus putting TCSPs in potential conflict with AML guidelines. Additionally, in some jurisdictions,

lawyers and other professionals fulfill the role that TCSPs play elsewhere, i.e., creating and administering trusts and companies to manage client assets (such as homes and cars) in jurisdictions other than those in which they live.

Although the vast majority of companies and trusts are used for legitimate purposes, the types of legal relationships formed by TCSPs are commonly used in money laundering schemes.

FATF's report identifies the following vulnerabilities and red flags for the TCSP industry:

- Unknown or inconsistent application of regulatory guidelines regarding identification and reporting requirements
- Limited market restriction on practitioners to ensure adequate skills, competence, and integrity
- Inconsistent recordkeeping across the industry
- Potential for TCSPs to operate in an unlicensed environment
- Potential for a TCSP's CDD to be performed by other financial organizations, depending on the jurisdictional requirements

Potential indicators of money laundering in the TCSP industry include:

- Transactions that require the use of complex and opaque legal entities and arrangements
- The payment of consultancy fees to shell companies established in other jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies
- The use of TCSPs in jurisdictions that do not require TCSPs to capture, retain, or submit to competent authorities' information on the beneficial ownership of corporate structures formed by them
- The use of legal persons and legal arrangements established in jurisdictions with weak or absent AML/CFT laws and/or poor record of supervision and monitoring of TCSPs
- The use of legal persons or legal arrangements that operate in jurisdictions with strict secrecy laws
- Multiple intercompany loan transactions or multijurisdictional wire transfers that have no apparent or legal purpose

According to Transparency International, a global coalition working to end the injustice of corruption, it is important to focus on service providers, rather than the company or trust, because the latter is merely the tool through which money launderers operate. A company owned by criminals cannot protect itself, but service providers can, through diligence, reduce the risk of abusing the vehicles with which they have a relationship. For this reason, it is important for countries to regulate service providers.

Regulations should stipulate how the service provider conducts its business, including how directors selected by the provider meet their obligations as trustees or trusteeships. Gibraltar was the first jurisdiction to bring these activities under regulatory control by enacting legislation in 1989. Other offshore jurisdictions either have introduced some form of regulatory control or will in the future.

Regulations are not uniform; they range from a simple minimum capitalization requirement to full regulatory oversight. Often, the scope of the legislation is limited, excluding certain types of activities. Sometimes, the legislation bars regulators from gaining access to client files without client permission or a court order, thereby making checks on the adequacy of the license holder's CDD provisions extremely difficult. Furthermore, although some jurisdictions include service providers within their AML regulations—for example, by making compliance with the regulations a condition of licensing—many do not, leaving service providers free of any AML duties beyond those imposed upon the general public. According to Transparency International, because of these differing standards, individuals seeking to use a company or trust for criminal purposes can simply select a jurisdiction that lacks requirements or has only inadequate ones.

Real Estate

The real estate sector is frequently used in money laundering activities. Investing illicit capital in real estate is a classic method of laundering illicit funds, particularly in countries with political, economic, and monetary stability.

Escrow accounts, generally maintained by real estate agents, brokers, and other fiduciaries, are designed to hold funds entrusted to someone for protection and proper disbursement. Countless real estate and business deals are closed every day using escrow funds. They are attractive to money

launderers because of the many diverse transactions that can pass through them in any deal; escrow accounts can facilitate the movement of funds by cashier's checks, wire transfers, and company checks to seemingly legitimate individuals and companies. Given the high levels of activity expected in escrow accounts, money launderers can disguise illegal activity in an account while appearing to operate it legally.

Although cash purchases of real estate are becoming more prevalent, many transactions involve the deposit of a large check from the mortgagee, in addition to checks and cash required from the buyer at closing. A money laundering title insurance agent can make multiple deposits of cash on a given day at several banks in amounts under the currency reporting threshold, credited to different, nonexistent closings. The deposits appear to be typical business activities, but they might represent the steady accumulation of funds for the purchase of real property by a person wishing to hide the origin of funds. Ultimately, monies could be paid outright by the escrow agent as cashier's checks obtained by the agent as wire transfers, or as corporate or escrow checks to straw men or shell corporations.

Each closing also entails numerous routine disbursements for payment of the proceeds to the seller, payoff of the mortgage, real estate commissions, taxes, satisfaction of liens, and other payments. To a bank and other observers, the disbursement of funds at a closing might appear to be one legitimate set of transactions. Money laundering can be easily hidden because the size and volume of routine escrow account activity smooths out the "spikes" (i.e., the ups and downs in an account) and multiple deposits associated with money laundering.

The reverse situation can also occur in the real estate industry. A money launderer might find a cooperative property seller who agrees to a reported purchase price well below the actual value of the property and then accepts the difference in unreported cash. For example, a money launderer could purchase a $2 million property for $1 million and secretly give the balance to the cooperative seller. After holding the property for a time, the launderer could sell it for its true value of $2 million.

In the loan-back money laundering method, a criminal provides an associate with a specific amount of illegitimate money. The associate then provides a loan or mortgage back to the trafficker for the same amount, with all the necessary loan or mortgage documentation. This creates the appearance

that the trafficker's funds are legitimate. The scheme is reinforced through legitimately scheduled payments made on the loan by the traffickers.

FinCEN published *Suspected Money Laundering in the Real Estate Industry*, an assessment based on analysis of SAR filings. The report makes a distinction between fraudsters and money launderers. Lenders are likely to file a SAR when they are the target of failed or successful mortgage fraud schemes that threaten their organization's revenues. However, it can be extremely difficult to detect mortgage loan fraud perpetrated by money launderers, because money launderers project the image of legitimacy by integrating illicit funds through regular and timely payments. For example, only approximately 20 percent of SAR filings associated with the residential real estate industry reportedly described suspected structuring and/or money laundering.

The Australian Transaction Reports and Analysis Centre (AUSTRAC) identified real estate as a significant money laundering channel in Australia.

According to the brief, real estate is an attractive channel for laundering illicit funds because:

- It can be purchased with cash.
- The ultimate beneficial ownership can be disguised.
- It is a relatively stable and reliable investment.
- Value can be increased through renovations and improvements.

Money laundering through real estate can be relatively uncomplicated compared with other methods and requires little planning or expertise. Large sums of criminal proceeds can be integrated into the legitimate economy through real estate investments in the placement and layering phases. Properties can also be sold for a profit or retained for residential, investment, or vacation purposes in the integration phase.

In Australia, common money laundering methods involving real estate include:

- Using third-party straw buyers described as "cleanskins"
- Using loans and mortgages as a cover for laundering, which might involve lump sum cash repayments to integrate illicit funds into the economy
- Manipulating property values to disguise undisclosed cash payments through overvaluing, undervaluing, or flipping through successive sales to increase value

- Structuring cash deposits used for the purchase
- Generating rental income to legitimize illicit funds
- Conducting criminal activity, such as the production of cannabis or synthetic drugs, at the purchased property
- Using illicit cash to make property improvements to increase the value and profits at sale
- Using front companies, shell companies, trusts, and other company structures to hide beneficial ownership and obvious links to criminals
- Using gatekeepers, such as real estate agents, conveyancers, and solicitors, to conceal criminal involvement, complicate the money laundering process, and provide a veneer of legitimacy to the transaction
- Investing by overseas-based criminals to conceal assets and avoid confiscation from authorities in their home jurisdiction

The report cites methods for detecting money laundering through real estate when transactions intersect with the regulated AML/CFT sector, such as when transactions involve financial organizations in the form of loans, deposits, and withdrawals. It also outlines red flags that should prompt further monitoring and examination, particularly when multiple indicators are present.

These red flags include:

- Various uses of cash to aggregate funds for property purchase, down payment, and loan repayment
- Multiple purchases and sales in a short period of time, possibly involving property overvaluation, undervaluation, or straw buyers
- Use of offshore lenders
- Unknown sources of funds for purchase, such as incoming foreign wires in which the originator and beneficiary customer are the same
- Ownership being the customer's only link to the country in which the real estate is being purchased

In its five-part Towers of Secrecy series published in 2015, *The New York Times* pierced the secrecy of more than 200 shell companies that have owned condominiums at the Time Warner Center, a high-end property located in the heart of Manhattan. In the investigative series, the newspaper found that

nearly one-half of the most expensive residential properties are purchased through shell companies throughout the United States. At the Time Warner Center, non-Americans own 37 percent of the condos, at least 16 of whom have been the subject of governmental inquiries, including for housing and environmental fraud. These owners have included government officials and close associates of officials from Russia, Colombia, Malaysia, China, Kazakhstan, and Mexico. They primarily used limited liability companies for the purchases. Often, signatures on the property documents were illegible, blank, or signed by a lawyer with the lawyer's contact information registered.

The paper states that there are no legal requirements for the real estate industry in the United States to identify beneficial owners or examine their backgrounds. In 2016 (subsequent to *The New York Times* series), FinCEN began issuing a series of geographic targeting orders (GTOs) to help law enforcement identify individuals acquiring luxury residential properties through limited liability companies and other opaque structures without the use of bank financing. During the 180 days of each outstanding GTO, US title insurance companies are required to identify the natural people behind shell companies used to pay all cash for high-end residential real estate in specified US metropolitan areas that exceed specified dollar amounts prescribed for each area. It is important to note that, in this context, "all cash" refers to transactions that do not involve traditional financing; it does not necessarily refer to the use of physical cash.

International Trade Activity

International trade activity is critical to an integrated economy and involves numerous components that can be manipulated for the benefit of money launderers and terrorist financiers. These components include banks, currency exchanges, free trade zones, cross-border payments, ports, invoices, goods, shipments, shell companies, and credit instruments that are often inherently complex transactions. Trade-based money laundering and the Black-Market Peso Exchange (BMPE) are two significant money laundering techniques that have proven successful in illicit finance. Typically, free trade zones are manipulated in both techniques.

Free Trade Zones

Free trade zones (FTZs) play an integral role in international trade. FTZs are designated geographic areas with special regulatory and tax treatments for certain trade-related goods and services. FTZs are often located in developing countries near ports of entry, but they are separate from traditional ports of entry and typically operate under different rules. Most major FTZs are also located in regional financial centers that link international trade hubs with access to global financial markets. Examples of FTZs are the Colón Free Trade Zone in Panama and the Shanghai Free Trade Zone (officially the China Pilot Free Trade Zone) in China.

According to FATF, systemic weaknesses for FTZs include:

- Inadequate AML/CFT safeguards
- Minimal oversight by local authorities
- Weak procedures to inspect goods and legal entities, including inadequate recordkeeping and information technology systems
- Lack of cooperation between FTZs and local customs authorities

The relaxed oversight in FTZs makes it more challenging to detect illicit activity and provides an opportune setting for trade-based money laundering schemes. Moreover, FATF noted that some FTZs are as large as cities, which

makes it difficult to effectively monitor incoming and outgoing cargo, as well as repackaging and relabeling. Some FTZs export billions of dollars annually but have few competent authorities available to monitor and examine cargo and trade transactions.

Trade-Based Money Laundering

When men's briefs and women's underwear enter a country at prices of $739 per dozen, missile and rocket launchers export for only $52 each, and full toilets ship out for less than $2 each, one should notice the red flags. These manipulated trade prices represent potential money laundering, tax evasion, and terrorist financing.

FATF defines trade-based money laundering (TBML) as the process of disguising the proceeds of crime and moving value by using trade transactions to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity, or quality of imports and exports. Moreover, TBML techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

Money launderers can move money out of one country by using their illicit funds to purchase high-value products and then exporting them at low prices to a colluding foreign partner, who then sells them in the open market at their true value. To give the transactions the appearance of legitimacy, the partners may use a financial organization for trade financing, which often entails letters of credit and other documentation.

TBML represents an important channel of criminal activity and, given the growth of world trade, it is an increasingly important money laundering and terrorist financing vulnerability. Moreover, as the standards applied to other money laundering techniques become increasingly effective, the use of TBML can be expected to become increasingly attractive.

According to the *Guidance Paper on Combating Trade-based Money Laundering,* developed by the Hong Kong Association of Banks, understanding the commercial purpose of any trade transaction is a key requirement in

determining its money laundering risk. The guidance refers to six ways to execute TBML:

1. **Overinvoicing and underinvoicing:**
    - **Overinvoicing:** This technique involves invoicing the goods or services at a price above the fair market price, so the seller (i.e., exporter) can receive value from the buyer (i.e., importer). In this scenario, the payment for the goods or services is higher than the value that the buyer receives when it is sold on the open market.
    - **Underinvoicing:** This technique involves invoicing the goods or services at a price below the fair market price. The seller can transfer value to the buyer, because the payment for the goods or services is lower than the value the buyer receives when the goods are sold on the open market.
2. **Overshipping or short-shipping:** There is a difference between the invoiced quantity of goods and the quantity of goods that are shipped, whereby the buyer or seller gains excess value based on the payment made.
3. **Ghost-shipping:** In fictitious trades, a buyer and seller collude to create documentation indicating that goods were sold and shipped, and payments were made, but no goods were actually shipped.
4. **Shell companies:** These companies are used to reduce the transparency of ownership in the transaction.
5. **Multiple invoicing:** Numerous invoices are issued for the same shipment of goods, thus allowing the money launderer to make numerous payments and justify them with the invoices.
6. **Black market trades:** In the BMPE, a domestic transfer of funds is used to pay for goods by a foreign importer.

Letters of credit are another vehicle for money laundering. Letters of credit are a credit instrument issued by a bank that guarantees payments on behalf of its customer to a third party when certain conditions are met. Letters of credit are commonly used to finance exports because exporters want assurance that the ultimate buyer of its goods will make payment, and this is given by the buyer's purchase of a bank letter of credit. The letter of credit is then forwarded to a correspondent bank in the jurisdiction in which the payment is to be made. The letter of credit is drawn on when the goods are

loaded for shipping, received at the importation point, clear customs, and are delivered. Letters of credit can be used to facilitate money laundering by transferring money from a country with lax exchange controls, thus creating the appearance that an import transaction is involved. Moreover, letters of credit can also serve as a façade when laundering money through the manipulation of import and export prices. Another method of illegally using letters of credit is in conjunction with wire transfers to bolster the legitimate appearance of nonexistent trade transactions.

The Asia/Pacific Group on Money Laundering (APG) cited the lack of reliable statistics relating to TBML as a major obstacle in devising strategies to tackle it. To assist in recognizing the multiple forms of TBML, the group enumerates specific characteristics and red flags associated with jurisdictions, goods, corporate structures, and predicate offenses.

It concluded that any strategy to prevent and combat TBML needs to be based on dismantling TBML structures, while allowing genuine trade to occur unfettered. It calls for an integrated, holistic approach, with an emphasis on interagency coordination and international cooperation to standardize data and statistics, create domestic task forces, deliver TBML-focused training, and conduct further research.

FinCEN issued an advisory on the use of funnel accounts and TBML. The advisory was the result of the possible impact of the 2010 Mexican law that restricted cash deposits of US dollars in Mexican banks. Subsequently, the restrictions were expanded to include similar deposits made at exchange houses (casas de cambio) and brokerages (casas de bolsa) in Mexico. Furthermore, additional guidance was issued by FinCEN based on bulk cash smuggling trends related to the restrictions, which indicated an increase in the use of funnel accounts to move illicit proceeds of Mexico-related criminal organizations.

FinCEN defines a funnel account as “an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.”

Red flags of possible funnel account activity include:

- An account opened in one US state receives numerous cash deposits of less than $10,000 (the currency reporting requirement) by unidentified

persons at branches outside the geographic region in which the account is held.

- Business account deposits take place in a different geographic region from where the business operates.
- Individuals opening or making deposits to funnel accounts lack information about the stated activity of the account, the account owner, or the source of the cash.
- A business account receives out-of-state deposits with debits that do not appear to be related to its business purpose.
- There are notable differences between the handwriting on the payee, amount, and signature lines on checks issued from an account that receives out-of-state cash deposits.
- Wire transfers or checks issued from a funnel account are deposited into, or cleared through, the US correspondent account of a Mexican bank.

Trade-based money laundering (Case example: Methods of money laundering)

The EU single market's significant trade activity and numerous borders make it vulnerable to trade-based money laundering (TBML) activities. The high volume of trade can enable goods to be moved freely across borders, giving criminals the opportunity to obscure transactions and transfer illicit funds.

Many TBML schemes involve the use of luxury vehicles and other goods to legitimize funds from illegal activities. Criminals use the system to add complexity to their activities and further layer funds. Sophisticated organized crime groups (OCGs) can use a variety of sectors to diversify their risk and expand into many jurisdictions.

In 2017, a joint investigation supported by Europol involving Spanish and Italian authorities identified Italian nationals with OCG links. They had created a network of companies to launder the proceeds of drug trafficking via TBML activity and legitimize the illegal proceeds. They faked invoicing to legitimize activities and used a tax fraud scheme to increase the criminal proceeds.

The scheme began with the purchase of luxury vehicles in Germany by legal entities established and owned by the criminals, using cash generated by illicit sources. Most of companies were shell companies with the sole purpose of supporting the scheme. Using these legal entities, the criminals created a fake paper trail for sales and purchases, including value-added tax (VAT) chains. Next, they used TBML activities to move and disguise the proceeds of crime. They also generated additional criminal proceeds by committing tax fraud by importing goods VAT-free. The criminals also convinced a legitimate supplier in Italy to annually deliver high numbers of vehicles, increasing the legitimacy of their activities.

In addition, import and export companies owned by the OCG were used to purchase other items, ranging from luxury watches to clothing and footwear. The watches were purchased in European countries before being supplied to drug traffickers in Morocco and the Netherlands. The lower value goods purchased in Hong Kong and mainland China were exported to Colombia and Morocco for onward sale.

The criminals used the TBML scheme for laundering criminal proceeds and generating additional proceeds of crime. The activity spanned several jurisdictions, making it difficult for authorities to identify and understand the magnitude of the scheme.

Key takeaways

- Criminals use international trade to disguise illegal activities.
- Shell companies and fake invoicing are common techniques.
- Joint investigations mitigate cross-border and jurisdictional challenges.
- Criminals add complexity to cross border trade by commingling with legitimate activity.

Black Market Peso Exchange

A form of TBML, the BMPE is a process by which money in the United States derived from illegal activity is purchased by Colombian peso brokers and deposited in US bank accounts established by the brokers. The brokers sell checks and wire transfers drawn on those accounts to legitimate businesses, which use them to purchase goods and services in the United States. Although the United States is prominently figured in BMPE, the process is not limited exclusively to that country.

Colombian importers created the BMPE in the 1950s as a mechanism for buying US dollars on the black market to avoid domestic taxes and duties on the official purchase of US dollars and imported goods purchased with dollars. In the 1970s, Colombian drug cartels began using the BMPE to convert drug dollars earned in the United States to pesos in Colombia. Why? It reduced their risk of losing their money through seizures, and they received their money faster, even though they paid a premium to the peso broker.

FinCEN reported that black market currency exchange systems have evolved beyond the Colombian BMPE method, mainly because of increased diligence by US banks. A common method used for the initial placement of illicit funds into the financial system is structured deposits in the form of cash, money orders, and other financial instruments. However, money launderers are using individuals and businesses that have control over numerous bank accounts at numerous banks to smuggle cash in bulk from the United States. The smuggled US dollars are deposited into foreign institutions—often in Mexico, but also in Central and South American countries—and wired back to the United States and other prominent trade countries as payments for international trade goods and services.

Black market peso exchange example

According to the US Department of Justice the following is a typical BMPE scenario involving the United States and Mexico:

> A peso broker works with an individual engaged in illegal activity, such as a drug trafficker, who has US currency in the United States that he needs to bring to Mexico and convert to pesos. The peso broker finds business owners in Mexico who buy goods from vendors in the United States, such as XYZ Inc., and need dollars to pay for those goods. The peso broker arranges for the illegally obtained dollars in the United States to be delivered to the US-based vendors, such as XYZ Inc., where they are used

to pay for the goods purchased by the Mexico-based customers. Once the goods are shipped to Mexico and sold by the Mexico-based business owner for pesos, the pesos are turned over to the peso broker, who then pays the drug trafficker in Mexico.

Links of TMBL and BMPE schemes (Case example: Methods of money laundering)

In February 2021, the operator of an international wholesale consumer electronics business based in the US pled guilty to participating in a conspiracy to operate an unlicensed money services business (MSB). The MSB operated primarily between Colombia and the US and was used to legitimize money transfers. A US Drug Enforcement Administration (DEA) investigation led to the arrests of the company CEO and six Columbian nationals, who were arrested in Columbia. As of this writing, the US government is seeking the extradition of these Columbian individuals.

The DEA found that the network ran operations in the US and Columbia that enabled drug traffickers to move funds into the banking system. They then laundered the funds and moved them across the border, using a black-market peso exchange (BMPE) scheme. Among the charges was operating an MSB without a license.

The BMPE and similarly structured schemes are sophisticated methods of trade-based money laundering. Cash-intensive businesses and cross-border activities are high risk for being used to facilitate this crime.

In January 2020, an investigation by the Offices of the United States Attorneys and the DEA discovered that drug dealers in the US were connected to Columbian drug cartels. These dealers generated US dollars by selling Columbian drugs in the US. The cartels needed to move their funds out of the US, without physically transporting USD across international borders or directly depositing large amounts of cash into the financial systems. They used the BPME scheme to clean the illegal funds.

Money brokers are essentially unlicensed MSBs. Operating primarily in Colombia, they were used to receive US dollars in the US via couriers or receipt of wires. They then paid out in Columbian pesos in Columbia for a commission.

The US based Agarwal Electronics Business exported consumer electronics globally, including to Columbia. Its CEO knowingly participated in the scheme and worked with the money broker by offering use of his bank account to receive the funds in the US. This account was then used to transfer the proceeds of drug sales to accounts in Middle and South America. Upon receiving the funds into his bank account, the CEO arranged for the export of the roughly equivalent value of electronics products to certain Colombian suppliers. They in turn arranged to pay for the products by delivering pesos to an individual in Colombia. This individual then delivered the funds to the money broker. This scheme enabled the funds to be remitted to Colombia without the need to report, declare, or smuggle them over the US border.

Key takeaways

- The BMPE scheme enabled the cartels to place the money into the banking system and move it across borders.
- A TBML scheme was used to pay the money brokers in Columbian pesos.
- Cash intensive business and cross border activity are at higher risk of being used to facilitate money laundering.

Complex TBML/BMPE schemes (Case example: Methods of money laundering)

In April 2015, FinCEN issued a GTO that lowered cash-reporting thresholds and implemented additional recordkeeping requirements for certain financial transactions for approximately 700 Miami-based electronics exporters. According to FinCEN, the GTO was designed to disrupt complex BMPE-related schemes employed by drug-trafficking organizations, (DTOs), including the Sinaloa and Los Zetas DTOs based in Mexico.

Law enforcement investigations revealed that many of these businesses are exploited by sophisticated TBML/BMPE schemes in which drug proceeds in the United States are converted into goods that are shipped to South America, sold for local currency, and ultimately transferred to drug cartels. The GTO was designed to enhance the transparency of the covered businesses' transactions.

Key takeaways

- DTOs take advantage of complex BMPE schemes involving the export of goods across the US/Mexico border to help move funds from the US back to the country where the DTO is based.
- Lower cash-reporting requirements can help enforcement agencies detect BMPE schemes and alert regulated organizations to potentially suspicious activity.
- Robust recordkeeping can help to detecting BMPE schemes, so that enforcement officers can access a regulated organization's transaction records.

Wildlife Trafficking

Wildlife trafficking is defined as the illegal trade, smuggling, poaching, capture, and collection of endangered species and protected wildlife. It also includes wildlife derivatives and byproducts, such as leather, food, medicines, and exotic pets. The illegal wildlife trade threatens the extinction of several animal and plant species. It is a practice that affects more than 7,000 species worldwide to satisfy the illegal market demands for endangered wildlife and its byproducts.

The three stages of wildlife trafficking include:

1. **Source:** The first stage involves the location where the initial trafficking activities occur, such as the jurisdiction in which poaching and initial transport takes place. Wildlife trafficking crimes are often facilitated by bribing corrupt officials and individuals with access to the targeted species. At the source location, the profits generated are often the lowest. Furthermore, source countries are potentially the most significantly affected by the illegal wildlife trade from the biodiversity and economic standpoints.
2. **Transit:** The second stage involves the movement of poached or illegally obtained wildlife goods that are disguised and consolidated with other items for transportation. These concealed items can clear customs

because of known weaknesses in customs controls and/or bribery of corrupt officials.

3. **Destination:** The final stage involves poached, illegally acquired or trafficked goods arriving at their final destination for sale. Because the sale of these products is illegal in some countries, they are often sold at in-person or online black markets, where profits for distributors are often the highest.

Organizations can combat wildlife trafficking by:

- Joining the United for Wildlife Financial Taskforce and signing the Mansion House Declaration
- Using current suspicious activity reporting mechanisms to report potential wildlife trafficking
- Reviewing United for Wildlife Financial Taskforce intelligence alerts and implementing policies and procedures to support the detection and reporting of wildlife trafficking
- Reviewing FATF's *Money Laundering and the Illegal Wildlife Trade* report for valuable insights and red flags

Risk Associated with New Payment Products and Services

The internet, new payment platforms, and electronic money (e-money) have changed the way people conduct business and transact with one another, as well as how consumers buy products and services. Small corner shops that were limited to servicing local consumers can now have a broader, global reach with an online business as well. Digital payment platforms have altered how consumers and the regulatory environment view merchants and funds transmission. The lower cost of technology; globally interdependent society; increasingly highly skilled, engineering-based workforce; and entrepreneurial drive have all contributed to the evolution of new payment products and services that expand the boundaries of how and where money is used. Generally, the risk posed by these new payment systems is relative to the functionality of the services and their funding mechanisms.

Prepaid Cards, Mobile Payments, and Internet-Based Payment Services

Alternative payment methods, including prepaid cards, digital wallets, and e-money continue to rise in popularity in the increasingly digital, fast-moving world. In October 2006, FATF first published a report that examined the ways in which money can be laundered through the exploitation of new payment methods, such as prepaid cards, internet payment systems, mobile payments, and digital precious metals. The report found that, although there is a legitimate market demand for these payment methods, money laundering and terrorist financing vulnerabilities exist. In addition, cross-border providers of new payment methods can pose more risk than providers strictly operating within a specific country. The report recommended continued vigilance to further assess the effect of evolving technologies on cross-border and domestic regulatory frameworks. Since 2006, FATF has

published additional guidance on new payment methods, typologies, and the risk-based approach.

Prepaid cards

Prepaid cards have the same characteristics that make cash attractive to criminals: They are portable, valuable, exchangeable, and anonymous. Typically, prepaid products require the consumer to pay in advance for future purchases of goods and services. Each payment is subtracted from the balance of the card or product until the total amount is spent.

Prepaid cards can be categorized as either open loop or closed loop. Open-loop prepaid cards, many of which are network branded by American Express, Visa, or MasterCard, can be purchased and loaded with money by one person and used like regular debit cards by the same person or another person to make purchases or ATM withdrawals anywhere in the world. Closed-loop prepaid products are of limited use for a specific purpose or service, such as with a certain merchant or retailer, whether online or at a physical location. A prepaid card can be either nonreloadable, which means it is purchased for a fixed amount that cannot be reloaded as the funds are depleted, or reloadable, which permits adding funds on the card to replace what was previously spent.

Although there are many different types of prepaid cards that are used in a variety of ways, the cards typically operate in the same way as a debit card and ultimately rely on access to an account. There might be an account for each card that is issued or, alternatively, a pooled account that holds the prepaid funds for all cards issued. The cards can be issued by, and accounts can be held at, a depository institution or a nonbank organization; pooled accounts are normally held by the issuer at a bank.

According to the FATF reports on this topic, the potential risk factors commonly associated with prepaid cards are:

- Anonymous cardholders
- Anonymous funding
- Anonymous access to funds
- High value limits and no limits on the number of cards individuals can acquire

- Global access to cash through ATMs
- Offshore card issuers that might not observe laws in all jurisdictions
- Use as substitute for bulk-cash smuggling

Following multiple high-profile money laundering and terrorist financing cases involving prepaid cards, including the 2015 Paris attacks, the European Union took steps to reduce the limits on prepaid cards under the Fourth Anti-Money Laundering Directive, which went into effect in 2017, and again in the Fifth Anti-Money Laundering Directive, which went into effect in 2020. According to the Fifth Directive, the monthly transaction limit and maximum amount that can be stored on prepaid cards not subject to due diligence is €150. Online transactions associated with such cards have similarly been limited to €50. Restrictions have also been placed on the use of prepaid cards that originate from outside of the European Union. The combined deployment of limits and geographic restrictions have helped to mitigate some of the greatest risk factors commonly associated with prepaid cards.

Electronic money

According to the JMLSG's sectoral guidance on preventing money laundering and combating terrorist financing, e-money is "a prepaid means of payment that can be used to make payments to multiple persons, where the persons are distinct legal or natural entities." E-money products can be card-based, app-based, or online account-based. They can be issued by financial organizations, building societies, and specialist e-money institutions. Examples of e-money include prepaid cards that can be used to pay for goods at a range of retailers and virtual purses that can be used to pay for goods and services online. All UK e-money institutions are regulated by the FCA and governed under the Electronic Money Regulations (2011), which require compliance with all AML/CFT and sanctions requirements. In the UK, this means all e-money institutions are subject to the Money Laundering Regulations 2017.

The guidance identifies several risk factors inherent in e-money for money laundering and terrorist financing, including:

- High transaction or purse limits
- The ability of a customer to hold numerous purses or cards

- E-money issuers using complex business models (e.g., “white-label” products and outsourcing, particularly to overseas jurisdictions), resulting in a complex AML/CFT control environment
- Certain merchant activity with high-risk businesses, such as gambling, which allows for the movement of higher amounts of funds
- Funding with unverified persons, whether customers or third parties
- Funding with cash that leaves no electronic trail to the source of funds, as well as the ability for cash withdrawal
- Funding with other e-money that lacks verified persons and/or source of funds
- Non-face-to-face transactional activity
- Features that increase the functionality of the card in terms of how to execute transactions, such as person-to-person, business-to-person, business-to-business, and person-to-business transactions

The guidance lists specific controls that e-money institutions should consider implementing in order to effectively mitigate the above risks, in addition to meeting standard AML/CFT obligations, including:

- Conducting robust oversight of outsourced functions
- Placing limits on storage values, transactions, and turnover
- Implementing transaction monitoring systems that are able to detect money laundering patterns and deviations from normal transaction patterns
- Implementing systems to detect individuals holding multiple purses, accounts, and cards, including across multiple e-money issuers
- Utilizing geolocation, device-related information, and IP addresses to identify discrepancies in customer activity from the information provided at onboarding (e.g., an individual onboarding in the United Kingdom, but only transacting from their device in Russia)

- Cooperating with merchants that accept e-money to better detect suspicious activity
- Instituting geographic restrictions on the use and function of e-money products, such as limiting use to the UK, EU, or other comparable jurisdictions with strong AML/CFT supervision

CDD is another important control that can help mitigate the risks associated with e-money. As noted above, there are some limits under which CDD is not required for prepaid card and e-money products. Outside of this, standard due diligence measures typically apply to e-money, although there are some circumstances in which simplified due diligence may be applied when the situation is sufficiently low-risk. When an e-money organization applies simplified due diligence, additional checks should still be considered to help mitigate fraud risk by establishing who controls a funding instrument. For example, some e-money issuers use a "micro-deposit," or a small charge on a customer's funding account, to help confirm the customer has access to the funding account and is not defrauding another individual.

E-money organizations are often just one party in a larger, more complex scheme that includes other banks, merchants, payment schemes, and payment processors. In these set-ups, e-money issuers must be satisfied that the due diligence measures being performed on the involved merchants align with sectoral guidance.

One concern with e-money is that it is offered predominantly in a non-face-to-face context. However, as noted in the FATF guidance paper *Digital Identity*, non-face-to-face onboarding can be just as robust, if not more so, as face-to-face onboarding when the appropriate systems and controls are in place to verify identities using reliable, independent sources.

The risks of payment services and e-money are also assessed by the United Kingdom's National Risk Assessment. In 2017 and 2020, the money laundering and terrorist financing risk level associated with payment services and e-money was "medium." The assessment noted certain typologies associated with e-money, such as the movement of illicit funds in and out of Eastern Europe, although it also noted the development of new controls. For example, "Strong Customer Authentication" adds extra layers of security checks to electronic payments to reduce the risk of fraud. The assessment concluded that the sector would continue to be monitored closely, given its novelty and likelihood to evolve.

Virtual Currency

Virtual currency (VC) is a medium of exchange, unit of account, and/or a store of value that operates in the digital space without legal tender status. VCs are distinguished from "fiat currency," or "real currency," which refers to government-issued currency that is typically accepted as the medium of exchange. Although a simplification, VCs often fall into two categories: centralized and decentralized. Centralized VCs have a centralized repository and a single administrator. They can be issued by a central government (e.g., the Bahamian Sand Dollar, the first fully launched central bank digital currency) or a non-government administrator (e.g., Facebook's Diem). Decentralized VCs (e.g., Bitcoin) have no repositories or administrators, but they work as a peer-to-peer media of exchange without the need for an intermediary.

According to FATF, VCs can also be distinguished between convertible VCs (e.g., Bitcoin, Ethereum, and Ripple), which have an equivalent value and can be exchanged in real currency, and non-convertible VCs (e.g., Reddit Coins and World of Warcraft Gold), which are intended to be specific to a particular domain.

VCs allow value to be transmitted anywhere in the world without the requirement of a centralized bank or institutional authority. In 2009, the Bitcoin ecosystem was developed as a cryptographic protocol to transfer value through a peer-to-peer network without reliance on a centralized banking structure. Since then, other coins, such as Ethereum, Dogecoin, and Litecoin, have become popular, and new coins are regularly being developed. Coins are units of value transfer that are established as a virtual currency. Much like any financial instrument, a coin derives its value from what another party is willing to trade for that item. For most coins, there is a value that is expressed in fiat currency that is based upon economic and market forces. Coins can be expressed as an equivalent value in each locale's specific currency.

One of the most significant concerns with regard to VCs and financial crime is the potential for anonymity. Some coins, such as Bitcoin, can be tracked through a public ledger. However, depending on the regulatory status of the exchanges and wallet providers involved, it can be difficult to identify who is behind a specific wallet address, where the funds originated, and the destination of the funds in the "fiat" space. Additionally, some coins, such as

Monero, ensure all users are anonymous, making it very difficult to trace funds.

FinCEN was one of the first FIUs to offer interpretative guidance on VCs and to clarify their regulatory status. FinCEN categorized participants in the ecosystem into three segments:

- A User is a person who obtains VC to purchase goods or services.
- An Exchanger is a person engaged as a business in the exchange of VC for real currency, funds, or other virtual currency.
- An Administrator is a person engaged as a business in issuing VC and who has the authority to redeem such virtual currency.

The guidance states that Administrators or Exchangers of VC are, unless exempted, MSBs engaging in money transmission. As such, they must comply with the registration, reporting, recordkeeping, and other regulations applicable to money transmitters, such as maintaining a compliant AML program.

In a typical transaction scenario, a User has an established virtual wallet or an account with an Exchanger to conduct a transaction. The User acquires VC from the Exchanger, which allows the User to transfer funds in and out of that account.

FinCEN consolidated and clarified its position by providing guidance for certain business models that involve convertible VCs. This guidance expanded how regulations would apply in different scenarios, including those involving different types of VC wallet providers, VC kiosks (often called “Crypto ATMs”), and decentralized (distribution) applications (“DApps”). DApps are software programs using distributed ledger technology that are not controlled by a single, identifiable administrator.

At a global level, FATF amended its Recommendations to explicitly require virtual asset service providers (VASPs)—providers of VCs—to be regulated for AML/CFT purpose as part of Recommendation 15. An interpretative note adopted on Recommendation 15 clarified how to consider other FATF Recommendations in the context of VCs and VASPs, including the application of a risk-based approach, supervision, and monitoring to VASPs, the implementation of AML/CFT controls within VASPs, and international cooperation on VC and VASP-related activity. This included expanding Recommendation 16 regarding the exchange of identifying information

between originators and beneficiaries, to cover VC transactions. This is commonly referred to as the “travel rule.”

FATF has since undertaken multiple reviews to assess the implementation of the revised FATF Recommendations. The Second 12-Month Review of the Revised FATF Standards, released in July 2021, noted that significant progress had been made globally in implementing the revised Recommendations, but that more work was still needed. Of 128 jurisdictions assessed in 2021, 70 (55%) had yet to implement the revised Recommendations into national law. Implementation of the travel rule was highlighted as being particularly difficult due to the absence of proper investment in the necessary technological solutions to facilitate full global compliance.

FATF published a list of red flag indicators to assist regulated organizations in identifying suspicious activity involving VCs. The report noted that the most common misuse of VCs was connected to sales of illicit substances, particularly through activity on the “dark web.” The second most common misuse was related to fraud, scams, ransomware, and extortion. The use of VCs to help layer and disguise the true origin of proceeds from professional money laundering networks is also becoming more common.

FATF updated its guidance for organizations working to design a risk-based approach to the treatment of VCs and VASPs that discourages blanket “de-risking” of virtual asset-related activity. The guidance provides additional risk indicators to consider in a VC context, particularly concerning the risks of peer-to-peer VC exchanges, as well as more information on the implementation of the FATF Recommendations, including the travel rule. The guidance also addresses how FATF standards apply to VCs tied to a specific fiat currency or commodity, otherwise known as stable coins. This followed an FATF Report to the Group of Twenty (G20) on the same subject. The guidance also clarifies when FATF standards might need to be applied to “decentralized finance,” or “DeFi,” products and services.

Use of virtual currency (Case example: Methods of money laundering)

In the early days of cryptocurrency exchanges, criminals operated in what was described as the “weak spot” of financial services. Criminal exchanges and operators were able to conduct a wide range of criminal activity, often with little enforcement action, due to limited primary and secondary legislation and regulation. Law enforcement also had limited capability to investigate and prosecute offenders.

In 2017, a ground-breaking US-led investigation into criminal users of BTC-e, a cryptocurrency trading platform, discovered that users were allowed to:

- Operate with high levels of anonymity, as user identification and verification details were not consistently required
- Obscure and anonymize transactions
- Openly discuss criminality on the BTC-e user chat
- Obtain advice from BTC-e on how to access illegally obtained money from drug sales

In December 2020, Paris courts sentenced Alexander Vinnik, founder of BTC-e, to five years in prison on money laundering charges.

Currently there exists a much wider understanding of the high risks presented by the use of cryptocurrency. This understanding has resulted in an array of global, cross-sector cooperation and regulation to prevent and prosecute the misuse of cryptocurrencies.

BTC-e was one of the first cryptocurrency exchanges and one of the world’s largest and most widely used digital currency exchanges.

In 2017 US authorities seized BTC-e, along with 38% of the users’ funds. Vinnik fled to Greece, where the authorities arrested him following US indictments for laundering US$4 billion worth of bitcoin (BTC).

Vinnik was linked to corrupt politicians, ransomware scams, identity theft schemes, and narcotics distribution rings. Greek authorities eventually extradited Vinnik to France in January 2020. Vinnik was found guilty by French authorities of money laundering as part of an organized crime group and sentence to 5 years in prison.

The activities in cryptocurrency laundering are often similar to those found in mainstream financial services. One difference is that the ultimate beneficiaries of cryptocurrency laundering need to convert their criminal cryptocurrency funds into criminal fiat funds to make them more widely usable, as part of the integration phase of money laundering.

Cryptocurrency laundering has prompted global regulators to ensure that local AML/CFT laws are updated and applicable to cryptocurrency service providers. The challenge with tracking virtual currencies is that they are identifiable only through a user's exchange account or cryptocurrency wallet address. In addition, the transactions are executed within seconds across exchanges and jurisdictions, and often from cryptocurrency to fiat currency.

FATF has identified cryptocurrency red flags. Individuals and organizations interacting with cryptocurrencies must understand the risks and red flags and incorporate them into their risk assessments.

Key takeaways

- Cryptocurrency exchanges can allow users to operate with high levels of anonymity and be used to obscure and anonymize transactions.
- Virtual currencies are challenging to track because they are identifiable only through a user's exchange account or cryptocurrency wallet address.
- Cryptocurrency transactions are executed within seconds across exchanges and jurisdictions, and often from cryptocurrency to fiat currency. The rapid changes introduced by cryptocurrencies require a consistent global approach in terms of law and regulation.
- Individuals and organizations interacting with cryptocurrencies must understand the risks and red flags and incorporate them into their risk assessment.

Virtual currency (Case example: Dark web)

In September 2020, the US Department of Justice announced the results of an international law enforcement operation targeting drug criminals who operated on the darknet. Operation DisrupTor's actions in the US and Europe resulted in the arrest of 179 darknet drug traffickers and other criminals who

engaged in tens of thousands of transactions involving illicit goods on both sides of the Atlantic. The operation also resulted in the seizure of over US$6.5 million in cash and virtual currency, mainly Bitcoin, 500 kilograms of drugs worldwide, and 63 firearms.

An unprecedented, coordinated international effort to disrupt opioid trafficking on the darknet, Operation DisrupTor, was jointly conducted by the US Joint Criminal Opioid and Darknet Enforcement (JCODE) and Europol. The operation identified numerous darknet vendor accounts through which criminals had been selling illicit goods on darknet market sites.

A common criminal pattern consisted of finding buyers on the dark web, accepting cryptocurrency as prepayment, and shipping drugs to customers' addresses through regular mail and other shipping services. One criminal group operating in the US city of Los Angeles completed more than 18,000 individual drug sales on several darknet sites. The group was also supplying other darknet vendors and street drug dealers.

The darknet offers its users anonymity, and cryptocurrencies, which are often the preferred method of payment on darknet sites, provide an additional way to veil transactions. According to the FBI, many drug users have grown more comfortable logging onto their computers and buying narcotics in a few minutes from their home than going to a street corner.

The darknet and its associated use of cryptocurrencies provides a large and expanding marketplace that crosses national borders to enable illicit activity. However, in an environment in which law enforcement action is identifying darknet operators and their activities, darknet users are increasingly searching for other ways to communicate, such as encrypted chat networks.

Key takeaways

- Cryptocurrency is the preferred payment method for purchasing illicit goods on the darknet.
- Law enforcement is increasingly capable of countering encryption and identifying anonymous data sources and transactions.
- Criminals will always search for new avenues of communication to avoid detection.

Corporate Vehicles Used to Facilitate Illicit Finance

A corporate vehicle is a legal entity that allows an administrator to perform commercial activities and manage assets on behalf of another person or company. Various forms of corporate vehicles can be used to facilitate the movement of illicit funds. For example, corporate vehicles can be misused for money laundering, bribery and corruption activities, sheltering assets, and tax evasion. Vehicles such as corporations, partnerships, and trusts are all effective methods to maximize anonymity of ownership as well as its actual purpose.

Public Companies and Private Limited Companies

In most jurisdictions, corporate structure is distinguished between public companies and private limited companies. For public companies, shares are freely available and traded publicly, there is usually no limit to the number of shareholders, information on ownership and its board of directors is publicly available, and the companies are subject to significant regulation. Conversely, private limited companies are not publicly traded, are restrictive in the number of shares, can be owned by one or many, and are subject to minimal regulatory oversight.

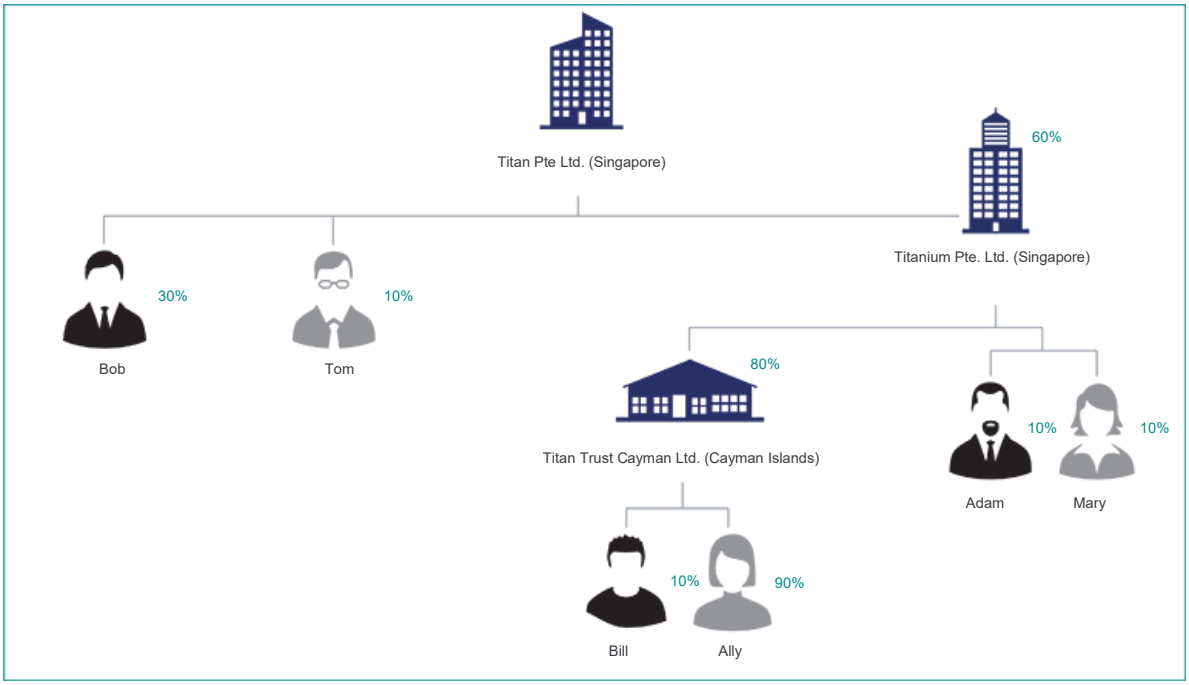
Limited liability companies (LLCs) are very common corporate vehicles that are subject to misuse. LLCs are an attractive vehicle because they can be owned or managed anonymously; virtually anyone can own or manage an LLC, including foreign persons and other business entities.

A member of an LLC is equivalent to a shareholder in a corporation. A manager of an LLC, on the other hand, is equivalent to an executive officer or member of the board of directors. An LLC can lack managers, in which case the members manage the LLC. FinCEN has undertaken a number of activities to better monitor LLCs, because not every state (especially US domestic

LLCs) undertakes the same measures and controls toward LLCs, particularly in the monitoring, recording, and reporting of managers, ultimate beneficiaries, and nominees.

International business corporations (IBCs) are entities formed outside a person's or business's country of residence, typically in offshore jurisdictions, for confidentially or asset protection purposes. IBCs permit the person to reduce transparency between the owner in her home country and the offshore entity where the company is registered. As a result, some benefits include asset protection, access to multiple investment markets, estate planning, legitimate tax benefits, and ability to serve as holding companies. The inherent risks with IBCs are that they are usually created in tax havens and typically require incorporation with a local agent, who may further reduce the transparency of the IBC (e.g., serving as a nominee owner or director) and facilitate opening accounts in the name of the IBC. Private investment companies are established and used in a similar manner; however, they are typically limited to holding investment assets in tax-neutral offshore financial jurisdictions.

Corporate vehicles example



Bearer shares in corporate formation

Bearer bonds, bearer stock certificates, and bearer shares are prime money laundering vehicles because they belong on the surface to the bearer. When bearer securities are transferred, because there is no registry of owners, the transfer takes place by physically handing over the bonds or share certificates. Basically, the person who holds the bonds or shares gets to claim ownership.

Bearer shares offer many opportunities to disguise their legitimate ownership. To prevent this strategy, FATF in its 40 Recommendations suggested that employees of financial institutions conduct EDD and ask questions about the identity of beneficial owners before issuing, accepting, and creating bearer shares and trusts. Financial institutions should also keep registries of this information and share it appropriately with law enforcement agencies.

Several FATF members do allow the issuance of bearer shares, maintaining that they have legitimate functions in facilitating the buying and selling of such securities through book entry transfers. They also can be used, according to some sources, for concealing ownership for tax optimization purposes.

Bearer checks are unconditional orders (i.e., negotiable instruments) that, when presented to a financial institution, must be paid to the holder of the instrument rather than to a payee specified on the order itself. Bearer checks are used in several countries. The financial institution is usually not obligated to verify the identity of the presenter of a bearer check unless the transaction exceeds a specific threshold. A non-bearer check may become a bearer instrument, payable to the individual who presents it, when the original payee has endorsed it.

Shell and Shelf Companies

Although shell companies can be created for legitimate purposes, they can also be established with the primary objective of claiming the proceeds of crime as legitimate revenue and/or to commingle criminal proceeds with legitimate revenue. The use of shell and shelf companies to facilitate money laundering is a well-documented typology, according to FATF.

FATF offers the following definitions:

- **Shelf company:** A corporation that has had no activity; it has been created and "put on the shelf." This corporation is then later sold to someone who prefers a previously registered corporation over a new one.
- **Shell company or corporation:** A company that at the time of incorporation has no significant assets or operations

FATF issued a report called *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers* in which it states that the ease with which corporate vehicles can be created and dissolved in some jurisdictions is of particular concern. This allows the vehicles to be used not only for legitimate purposes (e.g., business finance, mergers and acquisitions, and estate and tax planning), but also by financial criminals to conceal the sources of funds, while keeping their ownership concealed.

Shell companies can be set up in onshore as well as offshore locations, and their ownership structures can take several forms. Shares can be issued to a natural or legal person or in registered or bearer form. Some companies can be created for a single purpose or to hold a single asset. Others can be established as multipurpose entities. Shell companies are often legally incorporated and registered by the criminal organization, but they have no legitimate business. Often purchased "off the shelf" from lawyers, accountants, and secretarial companies, they are convenient vehicles to launder money. Sometimes, the stock of these shell corporations is issued in bearer shares, which means that whoever carries them is the purported owner. Tax haven countries and their strict secrecy laws can further conceal the true ownership of shell corporations. In addition, the information may be held by professionals who claim secrecy.

When FATF reviewed the rules and practices that impair the effectiveness of money laundering prevention and detection systems, it found that shell

corporations and nominees are widely used mechanisms to launder the proceeds from crime. The *Money Laundering in Canada* report offered four related purposes for establishing or controlling a shell company for money laundering:

1. Shell companies accomplish the objective of converting the cash proceeds of crime into alternative assets.
2. Through the use of shell companies, the launderer can create the perception that illicit funds have been generated from a legitimate source. Once a shell company is established, commercial accounts can be created at banks and other financial organizations. Especially attractive to money launderers are businesses that typically handle a high volume of cash transactions, such as retail stores, restaurants, bars, video arcades, gas stations, and food markets. Illicit revenues can then be deposited into bank accounts as legitimate revenue, either alone or commingled with revenue legitimately produced from the business. Companies also offer criminals legitimate sources of employment in the community, which in turn helps cultivate an image of respectability.
3. Once a shell company is established, a wide range of legitimate and/or fake business transactions can be used to facilitate the laundering process. These include lending money between criminally controlled firms, paying for fictitious expenses or salaries, disguising the transfer of illicit funds under the guise of payment for goods or services, purchasing real estate with the proceeds of crime, or disguising payments for real estate as mortgages issued by a shell company. As a medium between criminal organizations and other laundering vehicles, shell companies are flexible and can be tailored to a launderer's specific needs. For example, criminal organizations that launder money through real estate can incorporate real estate agencies, mortgage-brokerage firms, and development or construction companies to facilitate access to real property.
4. Shell companies can also be effective in concealing criminal ownership. Nominees can be used as owners, directors, officers, and shareholders. Companies in one country can also be incorporated as subsidiaries of corporations based in another country (especially a tax haven country with strict secrecy and disclosure laws), thereby significantly inhibiting investigations into their ownership. Shell companies can also be used to

hide criminal ownership in assets, by registering these assets, such as real estate, in the name of a company.

Criminal enterprises also use real businesses to launder illicit money. These businesses differ from shell companies in that they operate legitimately, offering industrial, wholesale, and retail goods or services.

The Canadian report identifies the following money laundering techniques used in conjunction with criminally controlled companies:

- **Using nominees as owners or directors:** To distance a company from its criminal connections, nominees are used as company owners, officers, and directors. Nominees will often, but not always, have no criminal record. Further, companies established by lawyers are often registered in the lawyers' names.
- **Layering:** In some cases, several companies are established, many of which are connected through a complex hierarchy of ownership. This method helps to conceal criminal ownership, facilitates the transfer of illicit funds between companies, and complicating any paper trail.
- **Loans:** Proceeds of crime can be laundered by lending money between criminally controlled companies. In one case, a drug trafficker had US$500,000 in a bank account in the name of a shell company. These funds were loaned to restaurants in which the drug trafficker had invested. This seemingly legitimate use of the funds helped make it appear as though the funds were being properly integrated into the economy. The US$500,000 was repaid with interest to avoid suspicion.
- **Fictitious business expenses/false invoicing:** Once a criminal enterprise controls corporate entities in different jurisdictions, it can employ a laundering technique known as double invoicing. An offshore corporation orders goods from its subsidiary in another country, and the payment is sent in full to the bank account of the subsidiary. Both companies are owned by the criminal enterprise, and the payment for goods is actually a repatriation of illicit money previously sent out of the country. Moreover, if the subsidiary has charged a high price for the goods, the records of the parent company will show a low level of profit, and it will pay less in taxes. Conversely, an offshore corporation buys goods from a parent company at an inflated price. The difference between the actual price and the inflated price is then deposited in the subsidiary's account.

- **Sale of the business:** When the criminal sells the business, he has a legitimate source of capital. The added benefit of selling a business through which illicit money circulates is that it will seemingly exhibit significant cash flow and, as such, will be an attractive investment that could realize a high selling price.
- **Buying a company already owned by the criminal enterprise:** This laundering method is most frequently used to repatriate illicit money that was previously secreted to foreign tax havens. Criminal proceeds from offshore are used to buy a company that is already owned by the criminal enterprise. In this way, the launderer successfully returns a large sum of money that had been secreted out of the country.
- **Paying out fictitious salaries:** In addition to claiming the proceeds of crime as legitimate business revenue, criminally controlled companies can help make participants in a criminal conspiracy appear to be legitimate by paying them salaries.

Trusts

Trusts are private fiduciary arrangements that allow a grantor, or settlor, to place assets for future distribution to beneficiaries. The grantor/settlor will usually appoint a third party, a trustee, to administer the assets in accordance with the instructions provided in the trust document. Trusts are often seen as separate legal entities from the grantor; as such, they are often useful for estate planning and asset protection purposes. The instructions usually state how the grantor/settlor wants the funds to be distributed and are limited only to a legal purpose.

Trusts fall into one of two categories: revocable and irrevocable. In revocable trusts, the grantor/settlor can terminate the trust. In irrevocable trusts, the grantor cannot terminate the trust once it is created. The flow of funds from the trust assets (i.e., the principal) to the beneficiaries can occur in several ways, including providing them with the income generated by the principal, providing fixed distributions of interest and/or principal, or putting conditions on distributions (e.g., completing certain levels of schooling). Trusts also name "remaindermen," who are designated to receive any residual assets after the conclusion of the trust's term (e.g., after the death of the grantor or the

beneficiaries). Trusts allow a significant amount of flexibility and protection and have been used legitimately for centuries.

The significance of trust accounts—whether onshore or offshore—in the context of money laundering cannot be overstated. It can be used in the first stage of converting illicit cash into less suspicious assets; help disguise the criminal ownership of funds and other assets; and form an essential link between different money laundering vehicles and techniques, such as real estate, shell and active companies, nominees, and the deposit and transfer of criminal proceeds.

In some jurisdictions, trusts can be formed to take advantage of strict secrecy rules in order to conceal the identity of the true owner or beneficiary of the trust property. They are also used to hide assets from legitimate creditors, protect property from seizure under judicial action, and mask the various links in the money flows associated with money laundering and tax evasion schemes. For example, an asset protection trust (APT) is a form of irrevocable trust that is usually created (i.e., settled) offshore for the principal purposes of preserving and protecting part of one's wealth from creditors. Title to the asset is transferred to a person named the trustee. APTs are generally used for asset protection and are usually tax neutral. Their ultimate function is to provide for beneficiaries. Some proponents advertise APTs as allowing foreign trustees to ignore US court orders and simply transfer the trust to another jurisdiction in response to legal action threatening the trust's assets.

Payments to the beneficiaries of a trust can also be used in the money laundering process, because these payments do not need to be justified as compensation or as a transfer of assets for services rendered.

Lawyers often serve as trustees by holding money or assets "in trust" for clients. This enables lawyers to conduct transactions and administer the client's affairs. Sometimes, illicit money is placed in a law firm's general trust account in a file set up in the name of a client, nominee, or a company controlled by the client. Trust accounts are also used as part of the normal course of a lawyer's duties in collecting and disbursing payments for real property on behalf of clients.

Terrorist Financing

After the terrorist attacks of September 11, 2001, the finance ministers of the Group of Seven (G-7) met on October 7, 2001, in Washington, D.C., and urged all nations to freeze the assets of known terrorists. Since then, many countries have committed to helping disrupt terrorist assets by alerting financial institutions about persons and organizations that authorities determine are linked to terrorism. The G-7 nations marshaled FATF to hold an “extraordinary plenary session” on October 29, 2001, in Washington to address terrorist financing. As a result, FATF issued the first eight of its Special Recommendations, which have since been incorporated into the current FATF Recommendations. (See the chapter "International AML/CFT Standards" for more detail.)

Recommendation 5 encourages countries to criminalize terrorist financing and the financing of terrorist organizations and individual terrorists with or without a link to a specific terrorist act, as well as ensuring these crimes are designated as money laundering predicate offenses. This designation allows the application of money laundering statutes to terrorist financing and the potential for greater prosecution and deterrence. Cutting off financial support to terrorists and terrorist organizations is essential to disrupting their operations and preventing attacks.

Differences and Similarities between Terrorist Financing and Money Laundering

Money laundering and terrorist financing are often mentioned together, but there are critically important differences between the two crimes. Many of the controls that businesses implement are intended to serve the dual purposes of combating money laundering and preventing terrorist financing. The controls instituted to combat money laundering also strengthen the ability to identify, deter, and disrupt terrorist financing. Of note, over half of the individuals investigated by US law enforcement for ties to terrorist

organizations and associated BSA records had engaged in suspected money laundering, including structuring.

But money laundering and terrorist financing are separate crimes. Although there is no workable financial profile for operational terrorists, there are key distinctions that can help compliance officers understand the differences and distinguish suspicious terrorist financial activity from money laundering.

The most basic difference between the two crimes involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. The purpose of laundering funds intended for terrorists is to support terrorist activities. The individuals responsible for raising the funds are not typically the beneficiaries of the laundered funds; rather, the money benefits terrorist activity. On the other hand, money laundering always involves the proceeds of illegal activity. The purpose of laundering is to enable the money to be used legally. The individuals responsible for the illegal activity are usually the ultimate beneficiaries of the laundered funds.

From a technical perspective, the laundering methods used by terrorists and other criminals are similar. Although it would seem logical that funding from legitimate sources does not need to be laundered, terrorist groups do need to disguise the link between them and their legitimate funding sources, in part to ensure the continued and uncompromised future use of sources. In doing so, the terrorists use methods similar to those of criminal organizations, such as cash smuggling; structuring; purchase of monetary instruments; wire transfers; and use of debit, credit, and prepaid cards.

The hawala system is an informal value-transfer system involving the international transfer of value outside the legitimate banking system. Based on a trusted network of individuals, this system has also played a role in moving terrorist-related funds. In addition, money raised for terrorist groups can be used for mundane expenses, such as food and rent; it is not always strictly used for the terrorist acts themselves.

Detecting Terrorist Financing

The National Commission on Terrorist Attacks Upon the United States determined that neither the September 11 hijackers nor their financial facilitators were experts in the use of the international financial system. The terrorists created a paper trail linking them to one another and their facilitators. Still, they were adept enough to blend into the vast international financial system without revealing themselves as criminals. The money laundering controls in place at the time were largely focused on drug trafficking and large-scale financial fraud; they were not sufficiently focused on the types of transactions made by the hijackers. Following 9/11, international efforts to detect and deter terrorist financing increased significantly. Conversely, in response to these efforts, terrorists and terrorist financiers have adapted, expanding and varying their methods of raising and moving funds, requiring increased innovation and vigilance by law enforcement and financial institutions.

In an attempt to clarify terrorist financing and offer recommendations to the global financial community, FATF issued guidance to identify techniques and mechanisms used in financing terrorism and described the general characteristics of terrorist financing. Its objective is to help organizations determine when transactions merit additional scrutiny so they can better identify, report (when appropriate), and ultimately avoid transactions involving funds associated with terrorist activity. FATF suggests that organizations exercise “reasonable judgment” in evaluating potential suspicious activity.

To avoid becoming conduits for terrorist financing, organizations must consider, among other things, the following factors:

- Use of an account as a front for a person with suspected terrorist links
- Appearance of an account holder’s name on a list of suspected terrorists
- Frequent large cash deposits in accounts of nonprofit organizations
- High volumes of transactions in accounts
- Lack of a clear relationship between the banking activity and the nature of the account holder’s business

FATF suggests that, with these scenarios in mind, organizations pay close attention to the classic indicators of money laundering, including dormant,

low-sum accounts that suddenly receive wire transfer deposits followed by daily cash withdrawals that continue until the transferred sum is removed, as well as lack of cooperation by a customer in providing required information.

Detecting terrorist financing (Case example: The Maute Group)

The threat of terrorism financing involves the risk that funds and other assets intended for terrorists are being raised, moved, stored, or used in or through a jurisdiction. Systemic vulnerabilities can allow these activities to go undetected, which can have dire consequences. Understanding the threat environment and systemic vulnerabilities can facilitate the detection and disruption of terrorism financing. Experience shows that ongoing engagement with foreign counterparts is particularly important in both detecting and assessing cross-border terrorist financing risks.

The 2018 Analyst Exchange Program (AEP) was a multinational project involving financial intelligence analysts from Australia, the Philippines, Malaysia, and Indonesia. The goal was to identify and understand the flow of funds, fighters, and material support to the radical Islamist Maute Group and associated groups in the Philippines prior to and during the Marawi Siege in 2017.

The AEP initiative identified money-moving networks, probable fund sources, networks used, and previously unknown financiers and facilitators that were utilized to finance terrorist groups in the Southern Philippines. The Maute terrorists were trained by the Islamic State of Iraq and Syria (ISIS) and gained experience in Syria and Iraq, or they were trained locally by a wealthy Muslim family, the Maute family. They were funded by:

- The Maute family
- ISIS
- The sale of shabu, a slang term for methamphetamine
- Anonymous mobile payments

During the AEP program, information was shared among the participants, including financial intelligence unit reports, transaction reports, and

intelligence from domestic authorities and the private sector. This information has supported ongoing investigations.

Key takeaways

- Terrorists need to raise, move, store, and use funds in order to sustain their operations.
- Countries must identify, assess, and understand terrorist financing risk as an essential part of dismantling and disrupting terrorist networks.
- Engaging with foreign counterparts is important in detecting and assessing cross-border terrorist financing risks.
- It's important to establish procedures and mechanisms to handle the exchange of sensitive information at an early stage in collaboration.

How Terrorists Raise, Move, and Store Funds

Global sanctions efforts have reduced funding to organizations from traditional state sponsors of terror, leading those organizations to seek supplemental sources of income to conduct their activities. In a December 2015 United Nations Security Council meeting, Secretary-General Ban Ki-moon told the Council: "Terrorists take advantage of weaknesses in financial and regulatory regimes to raise funds. They circumvent formal channels to avoid detection and exploit new technologies and tools to transfer resources. They have forged destructive and very profitable links with drug and criminal syndicates—among others. And they abuse charitable causes to trick individuals to contribute. Terrorists continue to adapt their tactics and diversify their funding sources," which he noted include raising money through the oil trade, extortion, undetected cash couriers, kidnapping for ransom, trafficking of humans and arms, and racketeering.

Use of Hawala and Other Informal Value Transfer Systems

Alternative remittance systems, or informal value transfer systems (IVTSs), are often associated with ethnic groups from Africa, Asia, and the Middle East. These systems commonly involve the international transfer of value outside the legitimate banking system and are based on trust. The systems are referred to by different names depending upon the country: “hawala” (an Arabic word meaning change or transform), “hundi” (a Hindi word meaning collect), “chiti banking” (referring to the way the system operates), “chop shop banking” (China) and “poey kuan” (Thailand).

Hawala was created centuries ago in India and China before Western financial systems were established to facilitate the secure and convenient movement of funds. Merchant traders wishing to send funds to their homelands would deposit them with a hawala broker, or hawaladar, who typically owned a trading business. For a small fee, the hawaladar would arrange for the funds to be made available for withdrawal from another hawaladar, typically also a trader, in another country. The two hawaladars would settle accounts through the normal process of trade.

Today, the process works much the same way, with people in various parts of the world using their accounts to move money internationally for third parties. In this way, deposits and withdrawals are made through hawala bankers rather than traditional financial institutions. The third parties are typically immigrants or visiting workers who send small sums to their homelands to avoid bank fees for wire transfers. Reasons for legitimate use of hawala and other IVTS include less expensive and faster money transmission, lack of banking access in the remittance-receiving country, cultural preference, and lack of trust in the formal banking system. There is usually no physical movement of currency and typically a lack of formality regarding verification and recordkeeping. The money transfer takes place by coded information that is passed through chits, couriers, letters, faxes, emails, text messages, and online chat systems, followed by some form of telecommunications confirmation. Almost any document that carries an identifiable number can be used by the receiver to pick up the values in the other country.

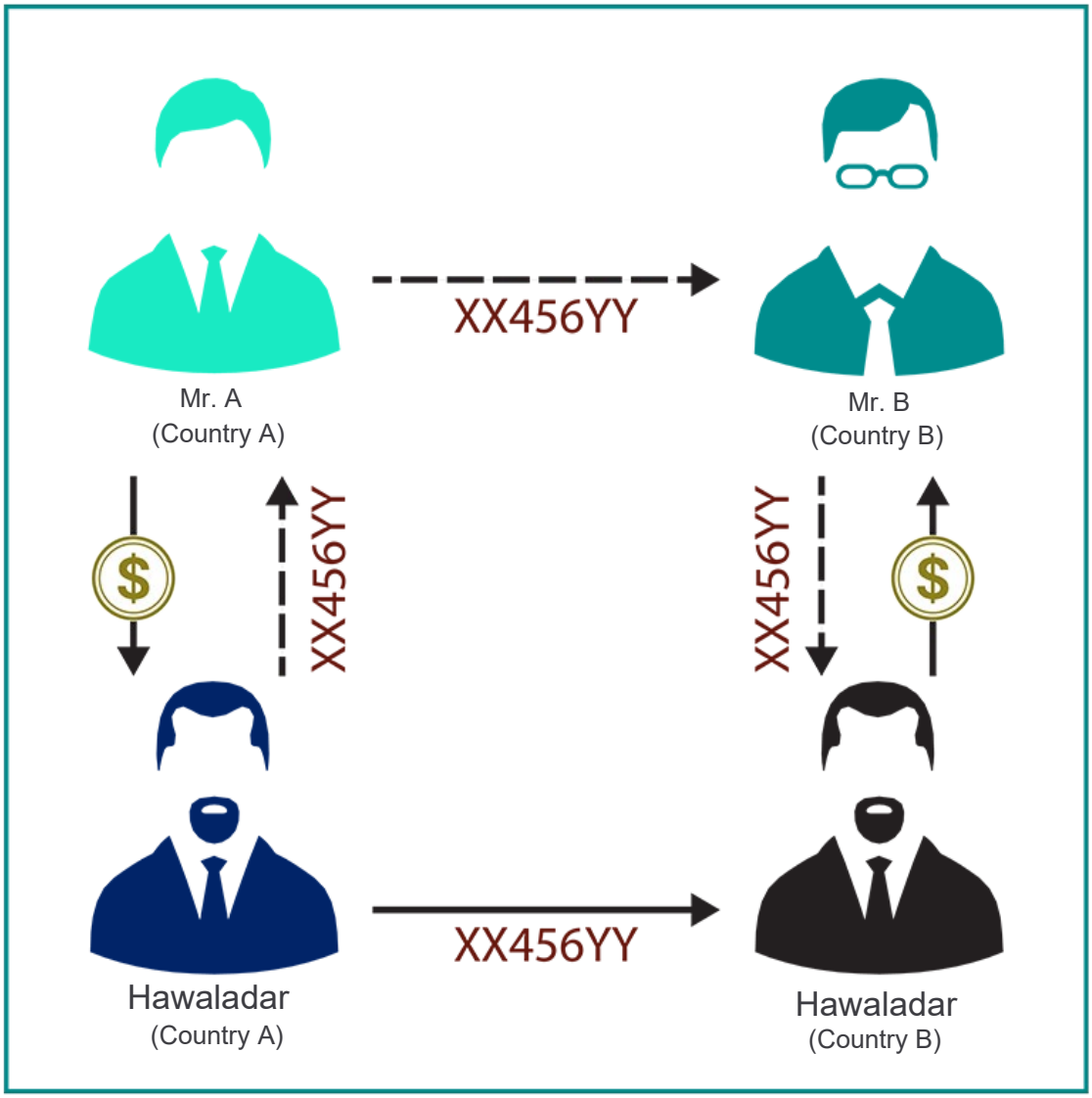
As AML/CFT measures have proliferated around the world, the use of hawala, which operates without governmental supervision, is believed to have

become more appealing to money launderers and terrorists. FATF has said that regulation and supervision of hawalas and other similar service providers remains a key challenge to authorities. It also notes that, as in other sectors, money laundering and terrorist financing risk increases the less regulation and supervision the hawala and similar service providers are subjected to. These providers are attractive to launderers because they leave little to no paper trail; the details of the customers who will receive the funds are communicated to the receiving brokers via telephone, fax, and email. Authorities have observed the use of advanced internet technologies by hawala and other similar agents and suspect they are exclusively using protected online services to conduct their activities and maintain their accounts, leaving no manual accounts.

Because hawala is a remittance system, it can be used at any phase of the money laundering cycle. It can provide an effective means of placement: When the hawaladar receives cash, he can deposit the cash in bank accounts. He will justify these deposits to bank officials as the proceeds of legitimate business. He may also use some of the cash received to pay for his business expenses, reducing his need to deposit the cash into a bank account. Hawaladars often operate within or in addition to a legitimate or front business to provide cover for the activity and commingle the funds in the business accounts.

A component of many layering schemes is transferring money from one account to another, while avoiding leaving a paper trail. A basic hawala transfer leaves little if any paper trail. Hawala transfers can be layered to make following the money even more difficult. This can be done by using hawaladars in several countries and distributing the transfers over time.

Hawala transaction example



Hawala techniques can be used to convert money into almost any form, offering many possibilities for establishing an appearance of legitimacy in the integration phase of the money laundering cycle. The money can be reinvested in a legitimate (or legitimate-appearing) business. A hawaladar could, for example, very easily arrange for the transfer of money from the United States to Pakistan and then back to the United States, apparently as part of an investment in a business there.

Hawalas are attractive to terrorist financiers because, unlike formal financial institutions, they are not consistently subject to formal government oversight and are not required to keep detailed records in a standard form. Although

some hawaladars do keep ledgers, their records are often written in idiosyncratic shorthand and are maintained only briefly. Al-Qaeda moved much of its money by hawala before September 11, 2001, using approximately 12 trusted hawaladars who almost certainly knew of the source and purpose of the money. Al-Qaeda also used unwitting hawaladars who probably strongly suspected that they were dealing with al-Qaeda, but they were nevertheless willing to engage in the transactions.

Detecting terrorist financing (Case example: Use of hawala and other informal value transfer systems)

On August 18, 2011, Mohammad Younis pled guilty in Manhattan federal court to operating an unlicensed money transfer business between the United States and Pakistan. One of the money transfers was used to fund the May 1, 2010, attempted car bombing in New York City's Times Square by Faisal Shahzad, who is serving a life sentence in federal prison. From January to May 2010, Younis provided money transmitting services to individuals in the New York City area by assisting in the operation of a hawala. On April 10, 2010, Younis engaged in two separate hawala transactions with customers who traveled from Connecticut and New Jersey to meet with him in Long Island. In each of the transactions, Younis provided thousands of dollars in cash to the individuals at the direction of a coconspirator in Pakistan, but without knowledge of how the customers were planning to use the funds. At no time did Younis have the license to operate a money transmitting business from either state or federal authorities.

One of the individuals to whom Younis provided money was Shahzad, who on June 21, 2010, pled guilty to a 10-count indictment charging him with crimes relating to his attempt to detonate a car bomb in Times Square on May 1, 2010. During the course of his plea allocution, Shahzad acknowledged receiving a cash payment in April 2010 in the United States to fund his preparations for the bombing. According to Shahzad, the April cash payment was arranged in Pakistan by associates of the Tehrik-e-Taliban, the militant extremist group based in Pakistan that trained him to make and use explosive devices. On September 15, 2010, Younis was arrested by the FBI and other agents of the

New York Joint Terrorism Task Force. Younis pled guilty to one count of conducting an unlicensed money transmitting business.

Key takeaways

- Unlicensed money transfer businesses, or hawalas, can be used to easily transfer sums of funds from high-risk jurisdictions at the direction of an unidentified third party.
- Hawalas can be particularly useful for moving funds for illicit purposes, especially when a hawaladar is unlicensed and not subject to AML/CFT requirements.
- The combination of the ease with which funds can be moved to and from high-risk jurisdictions and the limited level of scrutiny applied to transactions makes hawala especially attractive for terrorist financing.

Use of Charities and Nonprofit Organizations (NPOs)

After the September 11, 2001, attacks, the US government initiated the Terrorist Finance Tracking Program (TFTP) to identify, track, and pursue the funding sources of terrorist groups. Through the TFTP, the US government has uncovered and shut down over 40 designated charities that were used as potential fundraising front organizations.

Knowingly or not, charitable organizations have served as vehicles for raising and laundering funds destined for terrorism. As a result, some charities, particularly those with Muslim connections, have experienced a large drop in donations or have become targets of what they claim are unfair investigations and accusations. FATF acknowledges the importance of the nonprofit organization (NPO) sector to the global community. However, FATF found that more than a decade after the abuse of NPOs by terrorists and terrorist organizations was formally recognized as a concern, the terrorism threat to the sector remains. The sector continues to be misused and exploited by terrorist organizations through a variety of means.

Charities and NPOs have the following characteristics that are particularly vulnerable to misuse for terrorist financing:

- Enjoying the public trust
- Having access to considerable sources of funds
- Being cash-intensive
- Frequently having a global presence, often in or next to areas exposed to terrorist activity
- Often being subject to little or no regulation and/or having few obstacles to their creation

To help legitimate NPOs avoid ties to terrorist-related entities and regain public trust, FATF issued guidelines on best practices for charities in combating the abuse of NPOs. The guidance helps countries implement Recommendation 8 on NPOs in line with the risk-based approach, that is, to assist NPOs in mitigating terrorist-financing threats and assist financial organizations in the proper implementation of the risk-based approach when providing financial services to NPOs.

The objective of Recommendation 8 is to ensure that NPOs are not abused by:

- Terrorist organizations posing as legitimate entities
- Exploiting legitimate entities as conduits for terrorist financing
- Concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organizations

The best practices address identification and mitigation of risk by countries and NPOs alike, self-regulation by NPOs, and access of NPOs to financial services.

FATF recommends that NPOs maintain and be able to present full program budgets that account for all expenses, and conduct independent internal and external field audits, the latter to ensure funds are being used for intended purposes.

FATF recommends that charities use formal bank accounts to store and transfer funds so that they are subject to the banks' regulations and controls.

In turn, the banks where the accounts are established should manage NPOs like other customers, apply their KYC rules, and report suspicious activities.

The Charity Commission is an independent regulator of charities in England and Wales. Its role is to protect the public's interest in charities and ensure that charities further their charitable purposes for the public benefit and remain independent from private, government, and political interests. Its counter-terrorism strategy report dictates a four-strand approach to preventing abuse of charities by terrorist financiers, including:

1. Cooperation with government regulators and law enforcement nationally and internationally
2. Raising awareness in the sector of the risks charities face from terrorism
3. Oversight and supervision through proactive monitoring of the sector in areas identified as being at higher risk
4. Intervention when abuse, or the risk of abuse, related to terrorist activity is apparent

Detecting terrorist financing (Case example: Using NPOs)

Nonprofit organizations (NPOs) are an integral part of the global landscape. NPOs provide critically needed humanitarian aid around the world, especially to disadvantaged people in some of the most corrupt and under-governed territories, which often serve as "incubators" for terrorists. NPOs are at high risk for exploitation by terrorists.

The most commonly observed method of exploitation of NPOs to support terrorism involves the diversion of funds. In this typology, funds raised by NPOs for humanitarian programs are diverted to support terrorism at some stage of the NPO's business process; funds raised for charitable purposes are redirected to terrorists. Diversion occurs via internal actors, such as directing officials and staff, and via third-party associates.

Other less common methods of exploiting NPOs include affiliation with a terrorist entity, abuse of programing, support for recruitment, false representation, and sham NPOs.

The diversion of funds can be carried out by individuals who are internal to the organization. For example, a domestic NPO was raising funds for humanitarian relief in an area of conflict. The NPO used collection boxes outside religious institutions to solicit donations. The funds raised were held in a domestic bank account. The founder of the NPO was suspected of diverting the funds to facilitate terrorism rather than using them for the stated humanitarian activities. A law enforcement investigation resulted in the arrest of the founder of the NPO for terrorism facilitation offenses. In addition, US$60,000 in collected funds were seized.

The diversion of funds can also be perpetrated by individuals who are external to the organization. For example, a domestic NPO was established to support charitable work in foreign areas of conflict. An investigation by the national financial intelligence unit was initiated following suspicious transaction reporting. It revealed that locally collected funds were being transmitted to foreign-based charitable organizations. The investigation also uncovered that, once the funds were received by the foreign-based NPOs, they were systematically passed on to persons or organizations that were part of, or affiliated with, a known terrorist organization. Although there were established connections between the foreign-based charitable organizations and the terrorist organization, direct links between the domestic NPO and the terrorist organization could not be substantiated.

Key takeaways

- NPOs are at high risk for exploitation by terrorists.
- The diversion of funds occurs when funds raised for charitable purposes are redirected to support terrorist activity.
- The diversion of funds can be perpetrated by individuals internal and external to the organization.
- Diverted funds are used to support terrorist activities both domestically and abroad.

Detecting terrorist financing (Case example: NPOs and Islamic Defenders Front of Indonesia)

The nonprofit organization (NPO) sector has inherent vulnerabilities, which terrorist entities seek to exploit. A key risk that NPOs face is that they operate in the same vulnerable environments in which terrorists operate. One method of exploitation of NPOs to support terrorism is to form an operational affiliation between an NPO and a terrorist entity. These affiliations can range from informal personal connections involving NPO directors and terrorist entities to more formalized relationships.

In a typical affiliation, the NPO's internal actors, usually directing officials and staff, have established links to a terrorist entity. These internal actors are able to exercise influence over the operations of the NPO, which ultimately support terrorist entities. This can include the collection, transfer, retention, and expenditure of resources, and the delivery of programs. The affiliation involves every element of NPO operations.

The Islamic Defenders Front (FPI) was a hardline Islamist organization founded in Indonesia in 1998 by Muhammad Rizieq Shihab. The FPI originally positioned itself as the Islamic moral police against vice, and it conducted mostly illegal and unauthorized vigilante operations.

FPI gained support by appearing to be an NPO that provided voluntary-based welfare services in disaster-struck and poverty-ridden regions and neighborhoods. It provided schooling, food supplies, and other humanitarian aid. The Indonesian government alleged that Rizieq Shihab pledged FPI's allegiance to the Islamic State of Iraq and Syria (ISIS). Former FPI members were allegedly involved in the bombing of a cathedral in Makassar, Indonesia, in early 2021.

On December 30, 2020, the Indonesian government issued a joint ministerial decree banning FPI. The government claimed FPI had threatened Indonesia's national ideology, committed illegal raids and atrocities including terrorism, and allowed its organizational permit to expire. The government claimed that 29 members of the group had been convicted of committing acts of terror and that 100 FPI members had been convicted of other crimes. On January 6, 2021, Indonesia's financial intelligence unit, the Financial Transaction Reports

and Analysis Centre (PPATK) froze FPI's bank accounts to prevent the transfer of funds and use of funds from the accounts that were known or suspected to draw funds for illegal activity.

Key takeaways

- A key risk that NPOs face is that they operate in the same vulnerable environments in which terrorists operate.
- Affiliations between NPOs and terrorists can range from informal personal connections to more formalized relationships.
- In NPOs that are exploited by internal actors affiliated with terrorist entities, these individuals are able to exercise influence over the NPO's operations to ultimately support terrorist activities.
- Organizations must know their NPO customers, their staff members, and the individuals and entities with whom the NPO affiliates.

Emerging Risks for Terrorist Financing

FATF warns of several rising threats and vulnerabilities, including:

- Self-funding by foreign terrorist fighters (FTFs)
- Raising funds through social media
- New payment products and services
- Exploitation of natural resources

Self-funding by FTFs

Social media platforms, smartphone applications, and internet sharing sites provide terrorist organizations with global reach at little to no cost. FTFs and terrorist sympathizers can self-radicalize and communicate with terrorist organizations more efficiently than ever before. Often, the low cost associated with perpetrating a terrorist act on a soft target (i.e., a civilian, nonmilitary target that is relatively unprotected and thus vulnerable to terrorist attacks) makes it possible for such acts to be self-funded. Self-funding includes sources such as employment income, social assistance, family

support, and bank loans, which makes detection nearly impossible without the association of other aggravating terrorist financing indicators.

Former FBI Director James Comey stated, “Terrorists, in ungoverned spaces, disseminate poisonous propaganda and training materials to attract troubled souls around the world to their cause. They encourage these individuals to travel, but if they cannot travel, they motivate them to act at home. This is a significant change from a decade ago.”

Raising funds through social media

Social media platforms make it possible to build social and information-sharing networks like never before in human history. This technology presents a unique opportunity for terrorist organizations to communicate and raise money for their causes and the potential to reach into every home in every country in near real time. Terrorists have leveraged social media through methods such as crowdfunding and sharing of virtual and prepaid account information. These methods present unique difficulties for law enforcement, due to the increased dispersion of the activity and the need for cooperation from both financial institutions and social media platforms.

New payment products and services

(See the section "Risks Associated with New Payment Products and Services.")

Exploitation of natural resources

Terrorist organizations that hold or maintain control over territory or operate in a country with poor governmental control of the territory can take control of natural resources, such as gas, oil, timber, diamonds, gold and other precious metals, wildlife (e.g., ivory trading), and historical artifacts, or extort companies that extract those resources to both fund terrorist acts and support day-to-day activities. These resources themselves might be sold on the black market or to complicit companies, where they can then be integrated into the global trade sector. An awareness of geographies in which terrorist organizations operate and maintain control, knowledge of current commodity prices, and strong multijurisdictional partnerships are necessary to combat this method of terrorist funding, which has the potential to

generate vast sums. Red flags include the association of a customer with PEPs, complex legal entities structures with multiple internal transactions, and the rapid shipment of resources to distant jurisdictions.

Detecting terrorist financing (Case example: Islamic State and cryptocurrency)

Criminal convictions for terrorist funding remain relatively rare. As criminals, terrorists adapt and utilize new technology in the current operating environment. However, law enforcement expertise and skills also are becoming increasingly sophisticated, revealing funding methods and technologies used by terrorists. Law enforcement can use the unique investigative pathways presented by blockchain and cryptocurrencies to identify, arrest, and prosecute individuals and organizations that fund terrorism against states and individuals.

To combat the risks from terrorists using new technology, governments are enacting laws and guidance and working with exchanges and wider financial services to prevent misuse.

Terrorist organizations are continually exploring new ways to raise, store, move, and use funds. The same is true for individual criminals, or “lone actors,” who fund terrorist activity, often far from conflict zones. Increasingly, new technological capabilities open channels for financing terrorism, and the use of cryptocurrency is one of these.

In September 2021, at UK’s Birmingham Crown Court, Hisham Chaudhary, 28, was sentenced to 12 years’ imprisonment for one count of belonging to a proscribed terrorist group, two counts of entering terrorist fundraising arrangements, and four counts of disseminating terrorist publications.

As part of his role, from his home, Chaudhary received money from supporters and transferred over £50,000 abroad using Bitcoin. These funds paid smugglers to help captured ISIS militants escape from Kurdish-controlled prison camps in northern Syria. The court heard that Chaudhary immersed himself online on encrypted chat and video platforms, from which he spread terrorist propaganda and solicited funds. He deliberately developed his understanding and use of cryptocurrency to facilitate these transfers and used encrypted chat to communicate.

As is common, Chaudhary presented himself as a humanitarian and claimed his funding had charitable intent. Law enforcement, working with partners in cryptocurrency exchanges and financial services, rebutted this argument and proved his sustained support and funding of terrorists.

Within regulated organizations, the first line of defense is responsible for identifying and reporting suspicious cryptocurrency activity. Working in partnership across all sectors is the most effective way of preventing financial crime. This applies to terrorist financing as well, which is notoriously difficult to identify by one agency alone.

Key takeaways

- Terrorists are adapting to technology and increasingly conducting transactions digitally, including through cryptocurrency.
- Terrorists also use cyber-enabled tools to communicate.
- Law enforcement employs tools and investigative techniques to identify terrorist funding through misuse of cryptocurrency.
- Criminals often attempt to disguise terrorist funding as humanitarian activity.
- The first line of defense (LOD) is responsible for identifying and reporting suspicious cryptocurrency activity.

Detecting terrorist financing (Case example: Use of social media)

The global terrorist threat has shifted from being organizational to more individual-centric, and the threat environment has gone from being more centralized to decentralized. There are differences between the financial requirements of terrorist groups and individual terrorists; however, they all require funding to sustain their operations.

Social media can serve as a tool to facilitate and enable terrorist funding, recruitment, and propaganda. Terrorist groups, individual terrorists, and sympathizers are exploiting social media services to facilitate terrorist financing. Social media services are commonly used as communication

channels by terrorists and their financiers to solicit funding. One advantage of using social media platforms is that the large volume of legitimate funding activity on these platforms can mask the comparatively small amount of illegitimate activity.

According to the "Social Media & Terrorist Financing Report," by the Asia/Pacific Group on Money Laundering (APG) and the Middle East & North Africa Financial Action Task Force (MENAFATF), multiple platforms have been exploited by organized networks to collect donations for extremist organizations.

One case was detected through suspicious matter reports (SMRs) received by the Kuwait financial intelligence unit (FIU) from obliged reporting entities. Social media services, including Facebook, YouTube, Telegram, Twitter, and Instagram, were used to collect donations for extremist organizations. A privately owned website linked to a suspect was also used. Social media campaigns were created to solicit donations from the large number of followers on the sites. They provided bank account details and phone numbers for the people who collected the funds. Communication was undertaken via the various social media platforms and WhatsApp.

Various methods of funding were used, including cash, ATM deposits, and various internal and external transfers through banks, exchange companies, bank websites, and standing orders of payment and checks. Although communication was facilitated by social media platforms, no online payment platforms such as PayPal were used.

Some of the funds were used to purchase flights. The remaining funds were either transferred to other countries, where known terrorist organizations exist, or to countries adjacent to them.

Monitoring and surveillance of social media platforms by law enforcement can greatly enhance the detection of social media abuse by terrorists. Encryption, the process of encoding information, is a challenge that hinders law enforcement's ability to monitor and detect terrorist financing. Some examples of encrypted social media apps are WhatsApp, Telegram, Signal, and iMessage.

Key takeaways

- Social media can serve as a tool to facilitate and enable terrorist funding, recruitment, and propaganda.
- Social media services are commonly used as communication channels by terrorists and their financiers to solicit funding.
- Multiple social media platforms are exploited by organized networks.
- Monitoring and surveillance of social media platforms by law enforcement can greatly enhance the detection of social media abuse by terrorists.

International AML/CFT Standards

Financial Action Task Force

The pace of international activity in the AML field accelerated in 1989 when the G-7 nations launched FATF at its annual economic summit in Paris. With France serving as its first chair, this multinational group started working toward a coordinated effort against international money laundering.

Originally referred to as the G-7 Financial Action Task Force, today FATF serves as the vanguard in promulgating AML guidance to governmental bodies around the globe. The International Monetary Fund (IMF) and the World Bank also offer important perspectives to the field.

FATF has brought significant changes to the ways in which financial organizations and businesses around the world conduct their affairs. It also has brought about changes in laws and governmental operations.

The intergovernmental body is based at the Organisation for Economic Co-operation and Development (OECD) in Paris, where it has its own secretariat. FATF can be accessed online.

FATF Objectives

FATF's stated objectives are to "set standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system. Starting with its own members, the FATF monitors countries' progress in implementing the FATF Recommendations;

reviews money laundering and terrorist financing techniques and counter-measures; and promotes the adoption and implementation of the FATF Recommendations globally."

FATF fulfills these objectives by focusing on several important tasks, including:

- Spreading the AML message worldwide
- Monitoring implementation of the FATF Recommendations among its members
- Reviewing money laundering trends and countermeasures

Spreading the AML message worldwide

FATF promotes the establishment of a global AML and anti-terrorist financing network based on expansion of its membership, the development of regional AML bodies in various parts of the world, and cooperation with other international organizations.

Monitoring implementation of the FATF Recommendations among its members

With its fourth round of mutual evaluations, FATF adopted a new approach to assessing technical compliance with the Recommendations and determining whether a member's AML/CFT system is effective.

The new methodology was informed by the experience of FATF, FATF-Style Regional Bodies (FSRBs), the IMF, and the World Bank in conducting compliance assessments with earlier versions of the FATF Recommendations. Collectively, the technical compliance and effectiveness assessments provide an integrated analysis of the extent to which a country is compliant with the FATF Recommendations and how successful it is in maintaining a strong AML/CFT system. The methodology focuses on the technical compliance assessment, effectiveness assessment, and reviewing money laundering trends and countermeasures.

Technical compliance assessment

The technical compliance assessment evaluates the specific requirements of the FATF Recommendations, including how a member relates them to its relevant legal and institutional frameworks and the powers and procedures of its competent authorities. The focus is on the fundamental building blocks of an AML/CFT system.

For each Recommendation, assessors reach a conclusion about whether a country complies with the FATF standard. The result is a rating of five possible levels of technical compliance: compliant, largely compliant, partially compliant, noncompliant, and not applicable.

Effectiveness assessment

The goal of the effectiveness assessment is to assess the adequacy of a member's implementation of the FATF Recommendations and ensure there is evidence that a member is achieving a defined set of outcomes that are central to a robust AML/CFT system. The focus is on the extent to which the legal and institutional frameworks of the member are producing the expected results and protecting the financial system from abuse.

FATF defines effectiveness as "the extent to which the defined outcomes are achieved." Effectiveness is evaluated on the basis of 11 Immediate Outcomes:

1. Money laundering/terrorist financing (ML/TF) risks are known, and actions are coordinated to combat or thwart the proliferation of ML/TF.
2. International cooperation provides actionable information to use against criminals.
3. Supervisors regulate financial institutions and nonbank financial institutions (NBFIs) and their risk-based AML/CFT programs.
4. Financial institutions and NBFIs apply preventive measures and report suspicious transactions.
5. Legal persons are not misused for ML/TF, and beneficial ownership information is available to authorities.
6. Financial intelligence information is used by authorities in money laundering and terrorist financing investigations.

7. Money laundering offenses are investigated and criminally prosecuted, and sanctions are imposed.
8. Proceeds of crime are confiscated.
9. Terrorist financing offenses are investigated and criminally prosecuted, and sanctions are imposed.
10. Terrorists and terrorist organizations are prevented from raising, moving, and using money and are not permitted to abuse NPOs.
11. Persons and organizations involved in the proliferation of weapons of mass destruction are prevented from raising, moving, and using money.

Each of the 11 Immediate Outcomes represents a key goal of an effective AML/CFT system. They also feed into the three Intermediate Outcomes that represent major thematic goals of AML/CFT measures:

1. Policy, cooperation, and coordination to mitigate money laundering and terrorist financing
2. Prevention of proceeds of crime entering into the financial system and reporting of such when they do
3. Detection and disruption of ML/TF threats. For each individual immediate outcome, assessors reach conclusions about the extent to which a country is (or is not) effective and provide an effectiveness rating based on the extent to which the core issues and characteristics are addressed. Ratings include a high, substantial, moderate, or low level of effectiveness.

If a country has not reached a high level of effectiveness, assessors provide reasons why it fell below the standard and recommend measures the country should take to improve its ability to achieve the outcome.

Under the fourth round of FATF mutual evaluations, whether under regular or an enhanced follow-up status, follow-up assessments are conducted after five years.

FATF does not have the power to impose fines or penalties against recalcitrant member nations. However, in 1996, FATF launched a policy for managing nations that fail to comply with the FATF Recommendations, which it describes as “a graduated approach aimed at enhancing peer pressure.” This approach ranges from requiring the country to deliver a progress report at plenary meetings to suspension of membership.

In September 1996, Turkey became the first FATF member exposed to the peer pressure policy. Although a member since 1990, Turkey had yet to criminalize money laundering. FATF issued a warning to financial organizations worldwide to be vigilant in their business relations and transactions with people and entities in Turkey due to its lack of laundering controls. One month later, Turkey enacted a money laundering law.

Turkey became the first country to be added to the FATF list of Jurisdictions under Increased Monitoring. This list is often referred to the "greylist." Countries on the grey list have committed to resolve their identified strategic deficiencies and are subject to increased monitoring.

Reviewing money laundering trends and countermeasures

Faced with a financial system that has few geographic limitations, operates around the clock in every time zone, and maintains the pace of the global electronic highway, criminals are constantly searching for new points of vulnerability and adjusting their laundering techniques to respond to countermeasures introduced by FATF members and other countries. As such, FATF members are continually gathering information on money laundering trends to ensure the organization's Recommendations remain up to date. For example, in October 2013, FATF and the Egmont Group of financial intelligence units (FIUs) released a research report titled *Money Laundering and Terrorist Financing Through Trade in Diamonds,* which examined the vulnerabilities and risks of the "diamond pipeline" and described all sectors of the diamond trade, including production, rough diamond sale, cutting and polishing, jewelry manufacturing, and jewelry retailers.

Since its creation in 1989, FATF has been working under five-year mandates. In 2019, on FATF's 30th anniversary, FATF members adopted of an open-ended mandate. This mandate acknowledges that FATF's mission will continue to exist, as there are enduring concerns for the integrity of the financial system. In addition, a sustained political commitment to fight money laundering, terrorist financing, and proliferation financing is required. Since its establishment, FATF has focused its work on three main activities:

- Standard setting
- Ensuring effective compliance with the standards
- Identifying money laundering and terrorist financing threats

These activities will remain at the core of FATF's work. FATF will continue to build on that work and respond to new and emerging threats, such as proliferation financing and vulnerabilities in new technologies that could destabilize the international financial system.

FATF 40 Recommendations

A key element of FATF's efforts is its detailed list of appropriate standards for countries to implement. These measures are detailed in the 40 Recommendations, which were first issued in 1990 and have since been revised. FATF has also issued various Interpretative Notes, which are designed to clarify the application of specific recommendations and provide additional guidance.

After the events of September 11, 2001, FATF adopted and published the FATF IX Special Recommendations on terrorist financing, which were later merged into the 40 Recommendations.

FATF's Recommendations have become the world's blueprint for effective national and international AML/CFT controls. The IMF and the World Bank have recognized the FATF Recommendations as the international standard for combating money laundering and terrorist financing. The IMF, World Bank, and FATF use a common methodology to assess compliance with the FATF Recommendations.

The FATF 40 Recommendations provide a complete set of countermeasures against money laundering and terrorist financing, covering the following elements:

- Identification of risks
- Development of appropriate policies
- Criminal justice system and law enforcement
- Financial system and its regulation
- Transparency of legal persons and arrangements
- International cooperation

FATF recognizes that, because countries have different legal and financial systems, they cannot use identical measures to fight money laundering and

terrorist financing. The Recommendations set minimum standards of action for countries to implement according to their specific circumstances and constitutional frameworks. With its 2012 revision, FATF introduced risk assessment as the first recommendation, underscoring that assessing risk is the first step in combating money laundering and terrorist financing.

With its 2003 revisions of the 40 Recommendations, FATF expanded the reach of its global blueprint for preventing the illicit movements of funds. It introduced substantial changes intended to strengthen measures to combat money laundering and terrorist financing, which established further enhanced standards by which countries can better fight these crimes.

The most important changes made to the Recommendations in 2003 were:

- Expanded coverage to include terrorist financing
- Widened the categories of business that should be covered by national laws, including real estate agents, precious metals dealers, accountants, lawyers, and trust services providers
- Specified compliance procedures on issues such as customer identification and due diligence, including enhanced identification measures for high-risk customers and transactions
- Adopted a clearer definition of money laundering predicate offenses
- Encouraged prohibition of “shell banks,” which are typically established in offshore secrecy havens and consist of little more than nameplates and mailboxes
- Urged improved transparency of legal persons and arrangements
- Included stronger safeguards, notably regarding international cooperation in, for example, terrorist financing investigations

In 2012, the Recommendations were revised again, to incorporate the IX Special Recommendations on terrorist financing. The most important changes in this revision were:

- Creation of a Recommendation on implementing a process to identify, assess, monitor, manage, and mitigate AML/CFT risks using a risk-based approach
- Creation of a Recommendation on implementing a process to identify, assess, monitor, manage, and mitigate AML/CFT risks using a risk-based approach
- More information on assessing risks and applying a risk-based approach to all AML/CFT efforts
- Creation of a Recommendation for targeted financial sanctions related to the proliferation of weapons of mass destruction (WMD)
- More attention on domestic PEPs and individuals entrusted with prominent functions by international organizations
- New requirement for the identification and assessment of risks of new products prior to their launch
- New requirements on obtaining and sending accurate originator, intermediary, and beneficiary information in wire transfers (travel rule)
- New requirement for financial groups to implement group-wide AML/CFT programs and establish procedures for sharing information within the group
- Inclusion of tax crimes within the scope of designated categories of offenses for money laundering

The following table outlines the groups and topics of the FATF Recommendations by number.

FATF 40 Recommendations		
Group	Topic	Recommendation Number
I	AML/CFT Policies and Coordination • Assessing risks and applying a risk-based approach • National cooperation and coordination	1–2
II	Money Laundering and Confiscation • Money laundering offenses • Confiscation and provisional measures	3–4
III	Terrorist Financing and Financing of Proliferation • Terrorist financing offenses • Targeted financial sanctions related to terrorism and terrorist financing • Targeted financial sanctions related to proliferation • Nonprofit organizations	5–8

IV	Financial and Nonfinancial Institution Preventative Measures • Financial institution secrecy laws • Customer due diligence and recordkeeping • Additional measures for specific customers and activities • Reliance, controls, and financial groups • Reporting of suspicious transactions • Designated nonfinancial businesses and professions	9–23
V	Transparency and Beneficial Ownership of Legal Persons and Arrangements • Transparency and beneficial ownership of legal persons • Transparency and beneficial ownership of legal arrangements	24–25
VI	Powers and Responsibilities of Competent Authorities and Other Institutional Measures • Regulation and supervision • Operational and law enforcement • General requirements • Sanctions	26–35

VII	International Cooperation • International instruments • Mutual legal assistance • Mutual legal assistance regarding freezing and confiscation • Extradition • Other forms of international cooperation	36–40

Highlights of the 40 Recommendations include:

- **Risk-based approach:** Countries should start by identifying, assessing, and understanding the money laundering and terrorist financing risks they face. Then they should take appropriate measures to mitigate the identified risks. The risk-based approach allows countries to allocate their limited resources in a targeted manner in line with their own specific circumstances to increase the efficiency of preventive measures. Financial organizations should also use a risk-based approach to identify and mitigate their risks.
- **Designated categories of offenses:** The Recommendations specify crimes, referred to as "designated categories of offenses," which are considered money laundering predicates (i.e., crimes that offenders attempt to conceal through financial subterfuge that should constitute precursory offenses to money laundering). Countries should also put in place provisions to allow for the confiscation of the proceeds of crime or otherwise prevent criminals from accessing their criminal proceeds.
- **Terrorist financing and financing of proliferation:** Countries should criminalize terrorist financing, including the financing of terrorist acts, organizations, and individual terrorists, even if no terrorist activity can be directly attributed to the provision of financing. Countries should impose sanction regimes that allow them to freeze the assets of persons designated by the United Nations Security Council for involvement in terrorism or the proliferation of WMD. Countries should also establish

sufficient controls to mitigate the misuse of NPOs to provide support to terrorists.

- **Knowledge and criminal liability:** The Recommendations include the concept that the knowledge required for the offense of money laundering may be inferred from objective factual circumstances. This concept is similar to what is known in some countries as "willful blindness," or deliberate avoidance of knowledge of the facts. In addition, the Recommendations urge that criminal liability—or civil or administrative liability, when criminal liability is not possible—should apply to legal persons as well.
- **Customer due diligence measures:** Financial organizations should conduct CDD when they establish business relations, carry out occasional transactions or wire transfers above the specified threshold (US$1,000 and €1,000), have a suspicion of money laundering or terrorist financing, and have doubts about the veracity or adequacy of previously obtained customer identification information. Financial organizations must, using a risk-based approach:
    - Identify the customer and verify the customer's identity using reliable, independent source documents, data, and information. Establishing accounts in anonymous or obviously fictitious names should be prohibited.
    - Take reasonable measures to verify the identity of the beneficial owner, such that the financial organization is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this requirement includes understanding the ownership and control structure of the customer.
    - Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.
    - Conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken in the course of that relationship to ensure that they are consistent with the organization's knowledge of the customer, customer's business and risk profile, and, when necessary, source of funds.

- Maintain records of the above customer information and all transactions to enable compliance with requests from competent authorities.
- Rely on other parties to conduct CDD in certain circumstances; however, the relying institution remains liable for compliance with completing the required CDD.
- Establish a group-wide AML/CFT program for financial groups.

- **Additional CDD on specific customers and activities:** Some customer types and activities pose heightened risks, particularly the following:
  - **PEPs:** Appropriate steps must be taken to identify PEPs, including obtaining senior management approval of such business relationships, taking measures to establish the sources of wealth and funds, and conducting ongoing monitoring.
  - **Cross-border correspondent banking:** Appropriate steps must be taken to understand the respondent institution's business, reputation, supervision, and AML/CFT controls; obtain management approval of such relationships; document the responsibilities of each institution; mitigate risks associated with payable-through accounts; and ensure accounts are not established for shell banks.
  - **Money or value transfer services (MVTS):** Countries should ensure that MVTSs are licensed or registered and subject to appropriate AML/CFT requirements.
  - **New products, delivery mechanisms, and technologies:** Countries and financial organizations should assess the risks associated with the development of new products, business practices, delivery mechanisms, and technology. They should assess these risks prior to launching new products and take appropriate measures to mitigate the identified risks.
  - **Wire transfers:** Countries should require financial institutions to obtain and send required and accurate originator, intermediary, and beneficiary information with wire~~s~~ transfers and related messages (travel rule). Financial institutions should monitor wires for incomplete information and take appropriate measures. They should also monitor wires for the involvement of parties designated by the United Nations Security Council and take freezing actions or

otherwise prohibit the transactions from occurring. International wire transfers are liquid and difficult to retrieve, which make them susceptible to use as a tool by criminals to perform thefts or account takeovers to clear proceeds of crime. The requirements include virtual assets and exchanges.

    - **Suspicious activity reporting:** Financial organizations must report to the appropriate FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing. The financial organizations and employees reporting such suspicions should be protected from liability for reporting and prohibited from disclosing that they have reported such activity. One of the main concerns related to sharing of suspicious activity reports (SARs), the fact that a SAR has been filed, or the underlying SAR information is ensuring their confidentiality, which is critical to the effective functioning of the reporting regime.

- **Derisking:** Derisking refers to the phenomenon of financial organizations terminating or restricting business relationships with customers and categories of customers to avoid, rather than manage, risk. This practice is in line with FATF's risk-based approach. Derisking can result from concerns about profitability, prudential requirements, anxiety after a financial crisis, and reputational risk, among other reasons. The Recommendations only require financial organizations to terminate customer relationships, on a case-by-case basis, when the money laundering and terrorist financing risks cannot be mitigated.
- **Expanded coverage of industries:** The Recommendations expand the fight against money laundering by adding new nonfinancial businesses and professions to the list of financial institutions that are the usual focus of AML/CFT efforts. Expanding the scope of AML scrutiny is a key area on which many governments have been aiming their efforts, in response to an increased flow of illicit money. These designated nonfinancial businesses and professions (DNFBPs) include:
    - Casinos when customers engage in financial transactions equal to or above a designated threshold. At a minimum, casinos should be licensed. Authorities should prevent criminals from participating in

casino operations and supervise casinos to ensure compliance with requirements to combat money laundering and terrorist financing.

- Real estate agents when they are involved in transactions for clients concerning buying and selling properties
- Dealers in precious metals and stones when they engage in any cash transaction with a customer at or above a designated threshold
- Lawyers, notaries and independent legal professionals and accountants when they prepare or carry out transactions for clients concerning buying and selling real estate; managing client money, securities, and other assets; establishing or managing bank, savings, and securities accounts; organizing contributions for the creation or management of companies; creating, operating, and managing legal persons or arrangements; and buying and selling businesses
- Trust and company service providers when they prepare or carry out transactions for a client concerning certain activities (e.g., when acting as a formation agent of legal persons, acting as a director or secretary of a company, acting as a trustee of an express trust, or acting as a nominee shareholder for another person)

FATF also designated specific thresholds that trigger AML scrutiny. For example, the threshold that financial organizations should monitor for occasional customers is US$15,000; for casinos, including internet casinos, it is US$3,000; and for dealers in precious metals, when engaged in any cash transaction, it is US$15,000.

- **Transparency and beneficial ownership of legal persons and arrangements:** Countries should take appropriate measures to prevent the misuse of legal persons for money laundering and terrorist financing, including ensuring that information about the beneficial ownership and control of such legal persons is available to competent authorities, particularly with regard to legal persons who can issue bearer shares or have nominee shareholders or directors.
- **Powers and responsibilities of competent authorities:** Countries should oversee financial organizations to ensure they are implementing the FATF Recommendations and are not owned by or controlled by criminals. The supervisors should be given sufficient resources and powers to effectively

oversee financial organizations within their jurisdictions. DNFBPs also should be subject to oversight when they engage in certain financial activities. Countries should establish FIUs and provide law enforcement and investigative authorities with sufficient resources and powers to investigate money laundering and terrorist financing and seize or freeze criminal proceeds when found. Countries should implement measures to detect the physical cross-border movement of currency and bearer-negotiable instruments. The authorities should provide meaningful statistics, guidance, and feedback on AML/CFT systems.

- **International cooperation:** Several Recommendations address strengthening international cooperation. Countries should rapidly, constructively, and effectively provide the widest possible range of mutual legal assistance in money laundering and terrorist financing investigations, freezing and confiscation of criminal proceeds, extradition, and other matters. Countries should ratify United Nations conventions against significant crimes and terrorism.

FATF Members and Observers

FATF originally comprised 16 member jurisdictions. It has rapidly increased in membership and influence, and it now represents most major financial centers around the globe. Refer to the FATF-GAFI website for a current list of members and observers.

FATF membership criteria

The following criteria are applied when considering a country as a potential candidate for FATF membership:

1. The jurisdiction should be strategically important based on quantitative and qualitative indicators and additional considerations.
    - *Quantitative Indicators*
        - Size of gross domestic product (GDP)
        - Size of the banking, insurance, and securities sectors
        - Population

- *Qualitative Indicators*
    - Impact on the global financial system, including the degree of openness of the financial sector and its interaction with international markets
    - Active participation in an FSRB and regional prominence in AML/CFT efforts
    - Level of AML/CFT risks faced and efforts to combat those risks
- *Additional considerations*
    - Level of adherence to financial sector standards
    - Participation in other relevant international organizations

2. FATF's geographic balance should be enhanced by the jurisdiction becoming a member.

Process for FATF membership

Step 1–Engaging with the country and granting observership

- The country should submit a written commitment at the political/ministerial level:
    - Endorsing and supporting FATF Recommendations and the FATF AML/CFT Methodology 2013 (as amended from time to time)
    - Agreeing to undergo a mutual evaluation during the membership process for the purposes of assessing compliance with FATF membership criteria, using the AML/CFT methodology applicable at the time of the evaluation, as well as agreeing to submit subsequent follow-up reports
    - Agreeing to participate actively in FATF and meet all the other commitments of FATF membership, including supporting the role and work of FATF in all relevant fora
- The Plenary decides that a high-level visit to the country is warranted to verify the written commitment with the relevant ministers, representatives of the Parliament, and competent authorities. The visit will also determine whether the country will be in a position to undergo a successful mutual evaluation and achieve a satisfactory level of technical compliance,

including with the Recommendations essential for the establishment of a robust AML/CFT regime, such as Recommendations 3, 5, 10, 11 and 20, within 3 years. Consideration should also be given to the country's level of implementation of the essential Recommendations and its progress toward assessing and addressing its ML/TF risks, as described in Recommendation 1. The high-level visit should include the FATF President, selected members of the Steering Group, and heads of delegations. It is accompanied by the FATF Secretariat. The report of the high-level visit is presented at the following Plenary meeting.

- Based on the outcomes of the report of the high-level visit, the Plenary may decide to invite the country to participate in FATF as an observer, beginning with the next Plenary meeting. If the Plenary decides not to invite the country to attend FATF meetings as an observer, it may appoint a contact group to advise as to the appropriate time to extend such an invitation to the country. Then the contact group should engage with the competent authorities of the country to determine when the country will be able to undergo a successful mutual evaluation, as described in Step 2. The contact group is open to all FATF members and associate members and should include at least one member of the Steering Group. It is assisted by the FATF Secretariat. It will meet regularly and reports on the progress made by the country at each Plenary meeting.

Step 2—Carrying out a mutual evaluation, agreeing on an action plan, and granting membership

Membership is granted if the mutual evaluation is satisfactory. A mutual evaluation is not satisfactory if the country meets one of the following criteria:

Within a maximum of 3 years after being invited to participate in FATF as an observer, the mutual evaluation process for the country should be launched. During this period, a new contact group may assist the country to ensure that it is ready for its mutual evaluation.

- Has eight or more noncompliant/partially compliant (NC/PC) ratings for technical compliance
- Is rated NC/PC on any one or more of Recommendations 3, 5, 10, 11 and 20

- Has a low or moderate level of effectiveness for seven or more of the 11 effectiveness outcomes
- Has a low level of effectiveness for four or more of the 11 effectiveness outcomes

If the mutual evaluation is not satisfactory, but it is close to being satisfactory, the country should provide a clear commitment at the political/ministerial level to reach the expected results within a reasonable timeframe (i.e., a maximum of 4 years). A detailed action plan including the steps to be taken and timeframe is prepared by the country and reviewed by the second contact group before its adoption by the FATF Plenary.

At each FATF meeting, the Plenary closely monitors the implementation of the country's action plan. If it is not satisfied with the pace and/or extent of progress made, the Plenary can decide to apply to the country the enhanced measures listed under paragraph 77 of the procedures for the FATF fourth round of AML/CFT mutual evaluations. A country will not be granted full membership if it is rated NC/PC on any one or more of Recommendations 3, 5, 10, 11 or 20. Other than that, the Plenary may decide, at any time during the course of completion of the action plan and in light of the progress made by the country, to grant full membership before the action plan is completed.

Noncooperative Countries

Since its inception, FATF has had a practice of "naming and shaming" countries that it determines maintain inadequate AML controls or do not cooperate in global AML/CFT efforts. For years, FATF was engaged in an initiative to identify noncooperative countries and territories (NCCTs) in the global fight against money laundering. It developed a process to seek out critical weaknesses in specific jurisdictions' AML systems that obstruct international cooperation in this area.

On February 14, 2000, FATF published an initial report on NCCTs that listed the 25 criteria that help identify relevant detrimental rules and practices and that are inconsistent with the 40 Recommendations. It described a process whereby jurisdictions with such rules and practices can be identified and encouraged to implement international standards in this area.

The 25 distinct criteria are categorized in the following four broad areas:

1. Loopholes in financial regulations
    - No or inadequate regulations or supervision of financial organizations
    - Inadequate rules for the licensing or creation of financial organizations, including assessing the backgrounds of managers and beneficial owners
    - Inadequate customer identification requirements for financial organizations
    - Excessive secrecy provisions regarding financial organizations
    - Lack of efficient SAR reporting
2. Obstacles raised by other regulatory requirements
    - Inadequate commercial law requirements for registration of business and legal entities
    - Lack of identification of the beneficial owner(s) of legal and business entities
3. Obstacles to international cooperation
    - Obstacles to cooperation from administrative authorities
    - Obstacles to cooperation from judicial authorities
4. Inadequate resources for preventing and detecting money laundering activities
    - Lack of resources in public and private sectors
    - Absence of an FIU or equivalent mechanism

The goal of the NCCT process was to reduce the vulnerability of the financial system to money laundering by ensuring that all financial centers adopt and implement measures for the prevention, detection, and punishment of money laundering, according to internationally recognized standards. The next step in the NCCT initiative was the publication in June 2000 of the first review, which identified 15 NCCTs. The NCCT process ultimately involved 24 jurisdictions, including up to 19 jurisdictions at one time, until the jurisdictions eventually took the necessary steps to get off the list. At that point, FATF ceased the process.

The NCCT list has been replaced by a new process whereby FATF started identifying jurisdictions with deficiencies in their AML/CFT regimes. This new FATF process was in response to the G-20 countries' efforts to publicly identify high-risk jurisdictions and issue regular updates on jurisdictions with strategic deficiencies. It was also in response to criticism of the term "noncooperative," as many noncompliant jurisdictions simply lack the tools and infrastructure necessary to fight financial crime.

FATF's two public documents

FATF identifies these jurisdictions in two public documents issued three times a year.

The first document, *High-Risk Jurisdictions Subject to a Call for Action* (previously known as *Public Statement),* identifies countries and jurisdictions with strategic deficiencies that are so serious that FATF calls on its members and nonmembers to apply EDD and, in the most serious cases, countermeasures. This list is often referred to in the media as the "FATF blacklist."

The second document, *Jurisdictions under Increased Monitoring* (previously known as *Improving Global AML/CFT Compliance: On-going process*), identifies countries that are already actively engaging with FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. Once a jurisdiction is under increased monitoring, it means it has committed to swiftly resolve the identified strategic deficiencies within an agreed-upon time frame, while FATF keeps it under close scrutiny. This list is externally referred to as the "FATF greylist."

FATF encourages its members to consider the strategic deficiencies identified within these jurisdictions. If a country fails to make sufficient or timely progress, FATF can increase its pressure on the country to make more meaningful improvements by making it subject to a call for action. FATF also names jurisdictions that are no longer subject to its ongoing global AML/CFT compliance process. Typically, a country is considered to have made significant progress in improving its AML/CFT regime when it establishes a legal and regulatory framework for meeting its commitments in its action plan regarding the previously identified strategic deficiencies. However, the country must continue to work with the appropriate FSRB to address the items noted in its mutual evaluation report.

Review process

FATF's International Cooperation Review Group (ICRG) oversees the process of identifying and reviewing jurisdictions with strategic AML/CFT deficiencies. The process began in 2007 and was enhanced in 2009. It was updated in 2015 to reflect the revised FATF standards and mutual evaluation process. FATF reviews jurisdictions based on threats, vulnerabilities, and specific risks. Thus, a jurisdiction will be reviewed when it refuses to participate in an FSRB, does not allow its mutual evaluation results to be published in a timely manner, and/or has achieved poor results on its mutual evaluation. Results are considered "poor" when the jurisdiction has 20 or more noncompliant (NC) and partially compliance (PC) ratings for technical compliance, or a low level of effectiveness for 6 or more of the 11 immediate outcomes.

A jurisdiction that enters the ICRG review process as a result of its mutual evaluation results is given a one-year observation period to work with FATF or its FSRB to address deficiencies before possible public identification and a formal review by FATF. FATF then prioritizes the review of those countries that have more significant financial sectors, such as US$5 billion or more in financial sector assets. When FATF deems a jurisdiction's progress insufficient to address its strategic deficiencies, it develops an action plan with the jurisdiction to address the remaining strategic deficiencies. For all countries under review, FATF requires a high-level political commitment that the jurisdiction will implement the legal, regulatory, and operational reforms required by the action plan.

The Basel Committee on Banking Supervision

Introduction

The Basel Committee on Banking Supervision, established in 1974 by the central bank governors of the Group of Ten (G-10) countries, promotes sound supervisory standards worldwide. The Committee is the primary global standard-setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision, and practices of banks worldwide to enhance financial stability. The Committee is best known for its landmark publications on capital adequacy (Basel I, Basel II, and Basel III). The Committee's Secretariat is located at the Bank for International Settlements in Basel, Switzerland, and it is staffed mainly by professional supervisors on temporary assignment from member institutions.

MEMBERS OF THE BASEL COMMITTEE ON BANK SUPERVISION	
Country	Institution
Argentina	Central Bank of Argentina
Australia	Reserve Bank of Australia Australian Prudential Regulation Authority
Belgium	National Bank of Belgium
Brazil	Central Bank of Brazil
Canada	Bank of Canada Office of the Superintendent of Financial Institutions
China	People's Bank of China China Banking Regulatory Commission

European Union	European Central Bank European Central Bank Single Supervisory Mechanism
France	Bank of France Prudential Supervision and Resolution Authority
Germany	Deutsche Bundesbank Federal Financial Supervisory Authority (BaFin)
Hong Kong Special Administrative Region (SAR, China)	Hong Kong Monetary Authority
India	Reserve Bank of India
Indonesia	Bank Indonesia Indonesia Financial Services Authority
Italy	Bank of Italy
Japan	Bank of Japan Financial Services Agency
Republic of Korea	Bank of Korea Financial Supervisory Service
Luxembourg	Surveillance Commission for the Financial Sector
Mexico	Bank of Mexico Comisión Nacional Bancaria y de Valores
Netherlands	Netherlands Bank
Russia	Central Bank of the Russian Federation
Saudi Arabia	Saudi Central Bank
Singapore	Monetary Authority of Singapore
South Africa	South African Reserve Bank

Spain	Bank of Spain
Sweden	Sveriges Riksbank Finansinspektionen
Switzerland	Swiss National Bank Swiss Financial Market Supervisory Authority FINMA
Turkey	Central Bank of the Republic of Turkey Banking Regulation and Supervision Agency
United Kingdom	Bank of England Prudential Regulation Authority
United States	Board of Governors of the Federal Reserve System Federal Reserve Bank of New York Office of the Comptroller of the Currency Federal Deposit Insurance Corporation

OBSERVERS OF THE BASEL COMMITTEE ON BANK SUPERVISION	
COUNTRY	INSTITUTION
Chile	Central Bank of Chile Banking Financial Institutions Supervisory Agency
Malaysia	Central Bank of Malaysia
United Arab Emirates	Central Bank of the United Arab Emirates

History of the Basel Committee

Banking supervisors are generally not responsible for the criminal prosecution of money laundering in their countries. However, they play an important role in ensuring that banks have procedures in place, including strict AML/CFT policies, to avoid involvement with drug traffickers and other criminals, as well as generally promoting high ethical and professional standards in the financial sector. The Bank of Credit and Commerce International (BCCI) scandal in the early 1990s, the indictments and guilty pleas of former officials of the Atlanta branch of the Italian Banca Nazionale del Lavoro in 1992, and other international banking scandals prompted banking regulators in the richest nations to agree on basic rules for the supervision and operation of multinational banks.

In 1988, the Basel Committee issued a Statement of Principles, called *Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering,* in recognition of the vulnerability of the financial sector to misuse by criminals. This was the Committee's first AML/CFT commitment and a step toward preventing the use of the banking sector for money laundering. The statement set out principles with respect to:

- Customer identification
- Compliance with laws
- Conformity with high ethical standards and local laws and regulations
- Full cooperation with national law enforcement to the extent permitted without breaching customer confidentiality
- Staff training
- Recordkeeping and audits

These principles preceded AML legislation regarding the disclosure of customer information to enforcement agencies and protection from civil suits brought by customers for breach of confidentiality. Therefore, these principles stressed cooperation within the confines of confidentiality. Since 1988, the Committee has continued to publish papers in support of these commitments.

In 1997, the Basel Committee issued its *Core Principles for Effective Banking Supervision*, a basic reference for authorities worldwide. It stated that,

"Banking supervisors must determine that banks have adequate policies, practices, and procedures in place, including strict 'know-your-customer' rules that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements." It also urged nations to adopt FATF's 40 Recommendations. The Core Principles were prepared with the assistance of 15 non-G-10 nations, including Brazil, Chile, Hong Kong Special Administrative Region (SAR, China), Mexico, Russia, Singapore, and Thailand.

The *Core Principles for Effective Banking Supervision* has been periodically updated. The update in 2012 combined the core principles content with the assessment methodology to create a more comprehensive document. It also revised the structure of the 29 core principles, dividing them more clearly between principles for banking supervisors and for banks.

The revised standards include a core principle (BCP 29) that specifically addresses the abuse of financial services and emphasizes the need for adequate policies and procedures, including CDD rules.

The Basel Committee's KYC guidance centers on the use of due diligence requirements to mitigate the dangers of corrupt customers. Without due diligence, banks can be subject to reputational, operational, legal, and concentration risks, which can result in significant financial cost. Sound KYC policies and procedures are critical to protecting the safety and soundness of banks, as well as the integrity of banking systems.

The Committee has addressed the importance of KYC standards for supervisors and banks, essential elements of KYC standards, the role of supervisors, and implementation of KYC standards in a cross-border context.

Specific issues emphasized include:

- The four key elements of a KYC program:
    - Customer identification
    - Risk management
    - Customer acceptance policy
    - Ongoing monitoring
- Banks should not only establish the identity of their customers, but they should also monitor account activity to identify transactions that do not conform to the normal or expected transactions for that customer or type

of account. “To ensure that records remain relevant, there is a need for banks to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated.”

- Numbered accounts should not be prohibited, but they should be subjected to exactly the same KYC procedures as other customer accounts. KYC tests may be carried out by select staff, but the identity of customers must be known to an adequate number of staff if the bank is to be sufficiently diligent. “Such accounts should in no circumstances be used to hide the customer identity from a bank’s compliance function or from the supervisors.”
- Specific customer identification issues related to high-risk customers include:
    - Trust, nominee, and fiduciary accounts
    - Corporate vehicles, particularly companies with nominee shareholders or entities with shares in bearer form
    - Introduced businesses
    - Customer accounts opened by professional intermediaries, such as pooled accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds, and money funds
    - PEPS
    - Non-face-to-face customers (i.e., customers who do not present themselves for a personal interview)
    - Correspondent banking
- Banks should develop customer acceptance policies and procedures that describe the customer’s background, country of origin, business activities, and other risk indicators. They also should develop clear and concise descriptions of who is an acceptable customer.
- Private banking accounts should under no circumstances be allowed to escape KYC policies.

- Banks should make every effort to know the identity of corporations that operate accounts and, when professional intermediaries are involved, should verify the exact relationship between the owners and intermediary.
- Banks should use standard identification procedures when dealing with non-face-to-face customers and should never agree to open an account for persons who are adamant about anonymity.
- Periodic bank-wide employee training should be provided that explains the importance of the KYC policies and AML requirements.
- Internal auditors and compliance officials should regularly monitor staff performance and adherence to KYC procedures.
- Continued monitoring of high-risk accounts by compliance personnel should be conducted to obtain a greater understanding of the customers' normal activities and enable the updating of identification papers and detection of suspicious transaction patterns.
- Bank regulators should ensure that bank staff follow KYC procedures, review customer files and a sampling of accounts, and emphasize that they will take appropriate action against officers who fail to follow KYC procedures.

Customer identification is an essential element of an effective CDD program, which banks need in order to guard against reputational, operational, legal, and concentration risks. It is also necessary to comply with AML legal requirements and identify bank accounts related to terrorism. In February 2003, the Committee issued account opening and customer identification guidelines and a general guide to good practices based on the principles of the Committee's paper, Customer Due Diligence for Banks. This document, which was developed by the working group on cross-border banking, does not cover every eventuality; rather, it focuses on some of the mechanisms that banks can use to develop an effective customer identification program.

The need for rigorous CDD standards is not restricted to banks. The Basel Committee recommends that similar guidance be developed for all nonbank financial organizations and professional intermediaries of financial services, such as lawyers and accountants.

In October 2004, the Committee released another important publication on KYC, Consolidated KYC Risk Management, as a complement to its Customer

Due Diligence for Banks issued in October 2001. The 2004 paper examines the critical elements of effective management of KYC risk throughout a banking group and addresses the need for banks to adopt a global approach and apply the elements necessary for a sound KYC program to both the parent bank or head office and all of its branches and subsidiaries. These elements consist of risk management, customer acceptance and identification policies, and ongoing monitoring of high-risk accounts.

Recent guidance

In January 2014, the Basel Committee issued guidelines on Sound Management of Risks Related to Money Laundering and Financing of Terrorism that superseded previous publications on customer due diligence for banks and know-your-customer risk management. The goal of the guidelines was to support banking supervisors and banks in the implementation of the FATF Recommendations concerning AML/CFT within the wider context of banking supervision standards, drawing from the expertise of both organizations and working to avoid duplication.

The guidelines on management of risks related to money laundering and the financing of terrorism describe how banks should include these risks within their overall risk management framework. The guidelines state that prudent management of these risks, together with effective supervisory oversight, is critical in protecting the safety and soundness of banks and the integrity of the financial system. Failure to manage these risks can expose banks to serious reputational, operational and compliance risks among others.

The guidelines discuss the following controls for banks to implement:

- **Risk analysis and governance:** The first step in managing money laundering risks is to identify and analyze them, which leads to the design and effective implementation of appropriate controls. The analysis should include appropriate inherent and residual risks at the country, sector, bank, and business relationship levels, among others. The assessment of risk should be documented and made available to authorities, such as supervisors. This assessment is also useful in scheduling discussions with

other parties in the bank to help them see the risks and design the appropriate controls to mitigate them.

- Proper governance arrangements create a culture of compliance, with a strong compliance tone from the top. The board of directors plays a critical oversight role; as the senior-most management of the bank, the board should approve and oversee policies for risk, risk management, and compliance. To make informed decisions, the board also should have a clear understanding of the money laundering risks, including timely, complete, and accurate information related to the risk assessment. Along with senior management, the board should appoint a qualified chief AML officer with overall responsibility for the AML function. The board should provide this senior-level officer with sufficient authority so that, when issues are raised, they get the appropriate attention from the board, senior management, and business lines. This AML officer becomes the board's proxy for driving the day-to-day success of the bank's AML efforts. As such, the board should provide the AML officer with sufficient resources to execute his responsibilities to oversee compliance with the bank's AML program.
- **Three lines of defense:** The Committee describes three lines of defense in a bank's AML efforts: the line of business, compliance and internal control functions, and internal audit.
    1. **The line of business, or the first line of defense,** is responsible for creating, implementing, and maintaining policies and procedures, as well as communicating them to all personnel. It must also establish processes for screening employees to ensure high ethical and professional standards. It must deliver appropriate training on AML policies and procedures based on roles and functions performed so employees are aware of their responsibilities. To facilitate this, employees should be trained as soon as possible after being hired, with refresher training provided as appropriate.
    2. **The AML compliance and internal control functions**, as well as the larger compliance function and human resources and technology departments, comprise the second line of defense. In all cases, the AML officer is responsible for ongoing monitoring for AML compliance, including sample testing and review of exception reports, to enable the

escalation of identified noncompliance and other issues to senior management and, when appropriate, the board. The AML officer should be the contact point for all AML issues for internal and external authorities and should be responsible for reporting suspicious transactions. To enable the successful oversight of the AML program, the AML officer must have sufficient independence from the business lines to prevent conflicts of interest and unbiased advice and counsel. The officer should not be entrusted with the responsibilities of data protection or internal audit.

3. **The audit function, or the third line of defense,** should report to the audit committee of the board of directors (or a similar oversight body) and independently evaluate the risk management and controls of the bank. This is accomplished through periodic assessments, including the adequacy of the bank's controls to mitigate the identified risks, effectiveness of the bank's staff's execution of the controls, effectiveness of the compliance oversight and quality controls, and effectiveness of the training. The audit function must have knowledgeable employees with sufficient audit expertise. Audits should be conducted on a risk-based frequency; periodically, an enterprise-wide audit should be conducted. Audits should be properly scoped to evaluate the effectiveness of the program, including where external auditors are used. Auditors should proactively follow up on their findings and recommendations.

- **Customer due diligence and acceptance:** Banks should develop a customer acceptance policy to identify customers that are likely to pose a higher money laundering risk (e.g., PEPs) and relationships the bank will not accept (e.g., shell banks and those prohibited under economic sanctions, such as those imposed by the US Office of Foreign Assets Control). Banks should apply basic due diligence to all customers and increase the level of due diligence as the risks increase. Some customers may be eligible for simplified due diligence when the money laundering risk is low, in accordance with applicable law.

  When collecting information, a third-party database, or "KYC utility," can be particularly useful for gathering information on customers, especially assessing risk indicators. The Committee highlights several factors that

banks should consider when using a utility to perform due diligence, including:

- The utility specifies the date of the last update and when the information was last confirmed with the source.
- The utility clearly specifies the source of the information (e.g., the customer itself, a public registry).

Banks' CDD policies should address customer and beneficial owner identification, verification, and risk profiling. As part of this, banks should identify customers and verify their identities, as well as those of any beneficial owners. There are four main steps for verifying customers: (1) identification of the customer (whether an individual or a legal person) and any beneficial owners or authorized signatories; (2) assessment of the customer's risk profile information; (3) verification of the identity of the customer and any beneficial owners or authorized signatories, as required by applicable law, using reliable documentary and/or nondocumentary sources; and (4) further risk-based verification, such as verifying source of wealth and source of funds.

The minimum information to be collected on individuals includes the legal name, residential address, unique identification number or other identifier, and date and place of birth. Other potential information to be collected, based on risk, can include other names used, residency status, and business address. In order to accurately assess customer risk, certain information should be collected, such as occupation, income, expected use of the account, and products requested. Banks can use documentary and nondocumentary means to verify the information provided by the customer. Documentary methods can include using an unexpired government-issued photographic identification document or confirming a residential address on a utility bill or bank statement. Nondocumentary methods include using public registers, private databases, and other reliable and independent sources. Finally, further verification should be performed when a customer is considered high risk, such as verification of income sources, verification of employment, or a personal reference.

Banks should not establish a relationship or carry out transactions until the customer's identity has been verified, unless doing so would interrupt the normal conduct of business, in which case the bank should develop

appropriate controls while verification and CDD are performed. Verification of identity should be accomplished through reliable means. For beneficial ownership, banks may use a written declaration from the customer, but they should not rely solely on such declarations.

When CDD cannot be performed or a customer's identity cannot be verified, the bank should not open an account or should close such opened accounts and consider reporting the activity as suspicious to appropriate authorities. This applies to anonymous accounts as well; these should not be opened. If a bank allows for numbered accounts, these should not be allowed to serve as anonymous accounts; sufficient personnel should have full access to the information to ensure appropriate CDD on and oversight over these accounts.

- **Transaction monitoring systems and ongoing monitoring:** Because the transaction monitoring system is key to mitigating money laundering risk within a bank, the Committee recognizes that AML risks require more than just appropriate policies and procedures; banks must have adequate and appropriate monitoring systems. For most banks, this will involve an automated transaction monitoring system. If the bank does not believe it needs an automated transaction monitoring system, it should document the rationale for why it does not need one. The monitoring system should cover all accounts and transactions of the bank's customers, enable a trend analysis of activity, and identify unusual business relationships and transactions, particularly with regard to changes in the transactional profile of customers. The transaction monitoring system should allow the bank to gain a centralized knowledge of information, for example, organized by customer, by legal entity within a larger group, and/or by business unit. Although the guidance indicates a bank must have a system, it should be understood that this does not mean that there can only be one IT tool that will do all of the monitoring. Rather, the tools must be able to work together to enable the bank to gain an enterprise-level view of money laundering risk across the bank.

  A critical way to mitigate money laundering risk is to use the transaction monitoring system to conduct ongoing monitoring of customer activity, building on the information from risk assessments and customer profiles. This enables banks to satisfy their obligation to identify and report suspicious activity. Monitoring systems should be adapted to the risks

present in the bank, such as if the bank identifies a particular money laundering typology occurring within its jurisdiction.

- **Management of information:** Because one of the primary purposes of AML rules is to create records that enable law enforcement to trace financial transactions back to the people who conduct them, banks should retain records. Banks should record the documents they are provided when verifying customer and beneficial ownership identity, whether a photocopy of the document or information from a nondocumentary source, and enter all CDD information into their IT systems. The CDD information should be kept up-to-date and accurate, which will mean periodically assessing the information, generally on a risk-based frequency.

  Banks should also document decisions related to investigations of unusual activity, whether or not a decision is made to file a SAR. Banks should maintain all of these records, as required by law, for at least five years after closing the account. If an ongoing investigation is occurring, relevant CDD records should not be destroyed merely because the record retention period has expired.

- **Reporting of suspicious transactions and asset freezing:** Ongoing monitoring of accounts and transactions enables banks to identify unusual activity, refer unusual activity to an internal review function, eliminate false-positive alerts, and report suspicious activity in a timely and confidential manner. This process should be clearly described in policies and procedures and communicated to appropriate staff.

  When suspicious activity has been reported, the bank should take appropriate action regarding the customer, including raising the risk rating of the customer and/or deciding whether to retain the relationship (either the account or the entire relationship). In some cases, it might be appropriate to close out one account, but not the whole relationship, such as when a customer has both a checking account and an outstanding loan. Banks should screen new customers against applicable sanctions lists and the existing portfolio against changes to the sanctions list to identify relationships that may need to be frozen. Banks should have a means of properly freezing any assets identified as part of this process.

  The guidelines have been updated since their publication in 2014. In 2020, new text was added that set out specific principles and examples of

effective cooperation between prudential and AML/CFT supervisors. In many jurisdictions, prudential and AML/CFT supervision are handled by different authorities. For example, in the United Kingdom, prudential supervision is performed by the Prudential Regulation Authority, while AML/CFT supervision is performed by the Financial Conduct Authority. This situation can make cooperation on ongoing supervision and enforcement difficult to maintain. The 2020 update directly addresses this concern by sharing mechanisms on facilitating better cooperation at the domestic and international levels.

European Union Directives on Money Laundering

The European Union AML Directives are issued periodically by the European Parliament and implemented by member states as part of domestic legislation. The Directives are intended to prevent money laundering and terrorist financing and establish a consistent regulatory environment across the European Union, while allowing some flexibility based on local law. This is done by addressing the emerging money laundering and terrorist financing typologies, helping to close AML compliance gaps.

First Directive

The EU's First Directive of the European Parliament and of the Council, On Prevention of the Use of the Financial System for the Purpose of Money Laundering (91/308/EEC), was adopted by the Council of the European Communities in June 1991.

Like all directives adopted by the Council, it required member states to achieve the specified results, by amending national law, if necessary. This First Directive required members to enact legislation to prevent their domestic financial systems from being used for money laundering.

The unique nature of the EU as a community of states makes it fundamentally different from other international organizations. The EU can adopt measures that have the force of law even without the approval of the national parliaments of the various member states. In addition, European law prevails over national law in the case of directives. In this respect, EU directives have far more weight than the voluntary standards issued by groups such as the Basel Committee and FATF. Of course, the Directives apply only to EU member states and not to other countries.

The First Directive confined predicate offenses of money laundering to drug trafficking, as defined in the 1988 Vienna Convention. However, member states were encouraged to extend the predicate offenses to other crimes.

Second Directive

In December 2001, the EU agreed on a Second Directive (2001/97/EEC), which amended the First Directive to require stricter money laundering controls across the continent.

Member states agreed to implement it as national law by June 15, 2003; however, only Denmark, Germany, the Netherlands, and Finland met the deadline, with Ireland and Spain complying shortly afterward. Other member states eventually followed.

The following were the key features of the Second Directive:

- It extended the scope of the First Directive beyond drug-related crimes. The definition of criminal activity was expanded to cover not just drug trafficking, but all serious crimes, including corruption and fraud against the financial interests of the European community.
- It explicitly brought currency exchanges and money remittance offices under AML coverage.
- It clarified that knowledge of criminal conduct can be inferred from objective factual circumstances.
- It provided a more precise definition of money laundering to include:
    - The conversion or transfer of property with knowledge that it is derived from criminal activity or from participation in that activity, for the purpose of concealing or disguising the illicit origin of the property, or assisting anyone who is involved in the commission of the activity to evade the legal consequences of his action
    - Concealing or disguising the nature, source, location, disposition, movement, and rights with respect to or ownership of property, knowing that the property is derived from criminal activity or from an act of participation in that activity

- The acquisition, possession, or use of property, knowing when it is received that it was derived from criminal activity or from an act of participation in the activity
- Participation in, association to commit, the attempt to commit, and aiding, abetting, facilitating, or counseling the commission of any of the mentioned actions

- It widened the businesses and professions that are subject to the obligations of the Directive. Certain persons, including lawyers when they participate in the movement of money for clients, were required to report to authorities any fact that might indicate money laundering. Covered groups included auditors, external accountants, tax advisors, real estate agents, notaries, and legal professionals.

The Second Directive was a significant step forward because its applicability included many of the important financial centers of the world. It went well beyond similar standards issued by other organizations, such as the United Nations and even FATF.

Third Directive

A Third EU Directive, 2005/60/EC, On the Prevention of the Use of the Financial System for the Purposes of Money Laundering and Terrorist Financing, based on elements of FATF's revised 40 Recommendations, was adopted in 2005.

The EU expected the Third Directive to be implemented by member states by December 15, 2007. Although several countries did not meet this original deadline, the Directive was eventually implemented by all members.

In line with FATF's AML recommendations, the Third Directive extended the scope of the First and Second Directives by:

- Defining money laundering and terrorist financing as separate crimes. The Directive's measures were expanded to cover not only the manipulation of

money derived from crime, but also the collection of money and property for terrorist purposes.

- Extending customer identification and SAR reporting obligations to trusts and company service providers, life insurance intermediaries, and dealers selling goods for cash payments of more than €15,000
- Detailing a risk-based approach to CDD. The extent of due diligence that is performed on customers, whether simplified or enhanced, should be dependent on their AML/CFT risk.
- Protecting employees who report suspicions of money laundering or terrorist financing. This provision instructs member states to "do whatever is in their power to prevent employees from being threatened."
- Obligating member states to keep comprehensive statistics regarding the use of and results obtained from SARs, such as the number of reports filed, the follow-up given to those reports, and the annual number of cases investigated, persons prosecuted, and persons convicted
- Requiring all financial institutions to identify and verify (ID&V) the beneficial owner of all accounts held by legal entities or persons. "Beneficial owner" refers to the natural person who directly or indirectly controls more than 25 percent of a legal entity or person.

The Third Directive applies to:

- Credit institutions
- Financial institutions
- Auditors, external accountants, and tax advisors
- Legal professionals
- Trust and company service providers
- Estate agents
    - High-value goods dealers who trade in cash over €15,000 euros
- Casinos

The scope of the Third Directive differs from the Second Directive in that:

- It specifically includes the category of trust and company service providers.
- It covers all dealers trading in goods who trade in cash over €15,000.
- It expands the definition of financial institution to include certain insurance intermediaries.

There were three main points of contention regarding the Third Directive:

1. The definition of PEPs: The Third Directive defined PEPs as "natural persons who are or have been entrusted with prominent public functions and the immediate family members, or individuals known to be close associates, of such persons." Close associates must be identified only when their relationship with a PEP is publicly known or when the institution suspects there is a relationship. Finally, the Commission stipulated that persons should not be considered PEPs after one year of not being in a prominent position.
2. The Directive included lawyers among those professionals who are required to report suspicious activity.
3. The precise role of a comitology committee: The European Commission coined the term "comitology," which means the EU system that oversees the implementation of acts proposed by the European Commission.

Fourth Directive

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 On the Prevention of the Use of the Financial System for the Purposes of Money Laundering and Terrorist Financing took effect on June 26, 2015. Member states had two years from that date to adapt their national legislations accordingly. This Directive repealed the Third Directive and its predecessors.

Differences between the Fourth Directive and its predecessors include the following:

- Natural and legal persons trading in goods are covered to the extent that they make or receive cash payments of €10,000 or more (decreased from €15,000).
- The scope of obliged entities was enlarged from just casinos to all "providers of gambling services."
- CDD should be applied for transfers of funds exceeding €1,000. New definitions for:
    - Correspondent relationship
    - PEPs' family members and persons known to be close associates
    - Senior management and others
- Tax crimes relating to direct and indirect taxes are included in the broad definition of criminal activity, in line with the revised FATF Recommendations.
- An explanation of "financial activity on an occasional or very limited basis" was included.
- The European Commission must submit a report every two years on the findings of the risk assessment of money laundering and terrorist financing affecting the internal market.
- The EU executive is also in charge of identifying third-country jurisdictions that have strategic deficiencies with regard to AML and CFT (i.e., high-risk third countries).
- Special attention is given to PEPs. In this regard, EDD should be applied to every PEP, whether the individual is a domestic or third-country citizen. The risk these people pose is for at least 12 months, and measures they are subject to must also be applied to their family members and their known close associates.
- For groups (and their branches and subsidiaries), this Directive sets the criteria for adequate compliance related to CDD of third parties.
- New requirements regarding beneficial ownership information were introduced, particularly for trusts and similar legal arrangements. Subject to data protection rules, this information must be held in central registers in each member state and must be made available to competent authorities, FIUs, obliged entities, and any person with legitimate interest.

- Data in the statistics relevant to the effectiveness of systems to combat money laundering and terrorist financing were enlarged to include, for example, size and importance of sectors and the number of cross-border requests for information managed by FIUs.
- Obliged entities that are part of a group are required to implement group-wide policies and procedures and take measures proportionate to their risks. Criminals and their associates who are convicted in relevant areas are prevented from holding management functions and indirectly controlling certain obliged entities.
- With regard to penalties for breach of the provisions, the set of administrative sanctions and measures now ranges from "name and shame" to withdrawal of authorization. Pecuniary sanctions for natural persons are set to at least €5 million or 10 percent of the total annual turnover for entities.
- An entire section of the Directive is dedicated to the rules for cooperation between member state FIUs, the European Supervisory Authorities and the EU Commission.
- Because it is a directive and not a regulation, this legislative act gives some discretion to member states on the application of its provisions.
- At the national level, the Directive requests that member states conduct an AML/CFT risk assessment and designate a responsible authority. Moreover, they must ensure that obliged entities take appropriate steps to identify and assess their own risks. Nonexhaustive lists of potentially lower and

higher risks are provided for guidance in these risk assessments and are based on:

- Customer risk factors, such as public administrations versus cash-intensive businesses
- Risk factors related to products and services, transaction, and delivery channels, such as low premium insurance policies versus private banking
- Geographical risk factors, such as member states versus countries subject to sanctions.

Fifth Directive

Directive (EU) 2018/843 On the Prevention of the Use of the Financial System for the Purposes of Money Laundering and Terrorist Financing was put in place on July 9, 2018. The Fifth Directive further strengthens the EU's AML and CFT regime. It focuses on seven areas:

- **Beneficial Owners:** The Fifth Directive requires that national registers of beneficial ownership (excluding trusts) be publicly accessible. Regulated entities are required to provide "adequate, accurate, and up-to-date" information on their beneficial owners.
- **Cooperation and information sharing between regulators:** The Fifth Directive strengthens the cooperation and information sharing among financial supervisors across EU members.
- **High-risk third countries:** Additional monitoring on high-risk third countries is based on:
    - Countries on the FATF list and on the EU list
    - Autonomous assessment of additional countries that identifies the risk profile and level of threat to which each country is exposed and assesses the legal framework and its effective application in eight areas:
        1. Criminalization of money laundering and terrorism financing
        2. Customer due diligence (CDD) requirements, record keeping, and reporting suspicious transactions

3. Designated nonfinancial businesses and professions have the same CDD, record keeping, and reporting obligations.
4. Sanctions should be effective, proportionate and dissuasive.
5. Countries must ensure effective supervision.
6. International cooperation
7. Information about the beneficial owners of a legal entity and legal arrangements must be available.
8. Implement targeted financial sanctions (UN) to suppress terrorism.

The Fifth Directive added a streamlined EDD approach when transacting with high-risk countries, including:

- Collecting additional information on the customer, the beneficial owner and the nature of the business relationship, including source of funds and source of wealth
- Obtaining approval of senior management for business relationships
- Enhancing the monitoring of those entities, including obtaining information on the reasons for the intended or performed transactions

- **Prepaid Cards:** The Fifth Directive lowers the threshold when prepaid cards may be used anonymously to €150 from €250 when making in-store purchases and €50 when making purchases online.
- **Enhanced identification of PEPs:** The Fifth Directive introduces more efficient ways to identify PEPs by publishing a list of prominent PEPs gathered from each member state and accredited international organizations.
- **Extended scope of sectors and persons subject to AML/CFT obligations:** The Fifth Directive extends applicability of prior directives to the following sectors and persons:
  - Estate agents
  - Auditors, external accountants, and tax advisors

- Art traders
- Custodian wallet providers

- **Exchangers between virtual currencies (e.g., cryptocurrencies) and fiat currencies** will be required to have AML/CFT controls and need to be licensed or registered, while being supervised and monitored by relevant authorities. Virtual-to-virtual currency exchanges do not fall under this supervision.

Sixth Directive

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 On the Prevention of the Use of the Financial System for the Purposes of Money Laundering and Terrorist Financing became effective on December 3, 2020. Regulated entities operating in the European Union are required to be compliant by June 3, 2021. This Directive repealed the Fifth Directive and its predecessors.

The main purpose of the Sixth Directive is to create a better consistency on predicate offenses throughout the EU member states. The Directive includes the following changes:

- Harmonization of predicate offences against money laundering in all member states. The list consists of 22 predicate offences.
- Expanded regulatory scope by the introduction of “aiding and abetting,” “inciting,” and “attempting” as offences. This means that accomplices can face the same penalties as the individuals who profit directly from financial crimes.
- Criminal liability is extended to legal persons. In this manner, companies can be criminally liable for the actions of employees who engage in criminal activities.
- Tougher punishments for financial crime offenders, with the minimum jail sentence increasing from one year to four years. Legal entities will also

face tougher sanctions in the form of exclusion, permanent or temporary disqualification or closure, and placement under juridical supervision.

- Enhancement of cooperation and harmonization among member states addresses the issue of dual criminality, requiring member states to criminalize certain predicate offences.

  By harmonizing the predicate offences, there are no differences between how member states consider certain crimes. This eliminates the possibility that some member states would have laws that punish a specific crime, whereas other states would not punish the same crime. It creates equality and clarity, reducing the ability of criminals to pick the legislation within the EU that fits them best.

  The Sixth AML Directive further intensifies the fight against financial crime by stating that people who have willfully cooperated in a crime (vs. those who execute a crime) are also punishable by law. Simply said, when individuals are in some way involved in a financial crime, such as money laundering or terrorist financing, either by assisting or willfully ignoring it, they can still be prosecuted and face a jail sentence (of four years instead of one). Being involved in a financial crime can result in sentences for the involved individuals within an organization and enforcement actions against the organization as well. If an organization in part or as a whole aids financial criminals, the organization could be suspended or barred from certain activities. It is also possible that the organization could be put under supervision or even liquidated.

Seventh Directive

In July 2021, the EU Commission published a package of legislative proposals to further strengthen AML/CFT rules in the EU. This package might later be translated into the Seventh Directive. The aim of the proposals is to improve the detection of suspicious transactions and activities and close loopholes used by criminals to launder illicit proceeds and finance terrorist activities through the financial system. The package presents the following proposals:

- **Introduction of the EU centralized system of bank account registries:** This registry will provide access to banking information without further

authorizations or delays. The aim is to have a single, centralized access point for all national centralized bank account registries. It will allow enforcement authorities in every EU state to get immediate information about bank accounts opened in the European banks, as well as their beneficiaries.

- **Introduction of EU Central AML Authority (AMLA):** The proposals create a new EU authority that will transform AML/CFT supervision in the EU and enhance cooperation among FIUs. It will be the central authority, coordinating national authorities to ensure the private sector correctly and consistently applies EU rules. The expectation is that AMLA will be operational by 2024 and begin the work of direct supervision when the Directive has been transposed and new rules are effectuated.
- **Unification of AML/KYC rules in member states:** The European Commission wants EU member states to implement AML Directives much more quickly and have a "level playing field" (i.e., the same rules, documentation, and wording) for all member states. The European Commission thus intends to pass a regulation regarding unification of AML and KYC rules with direct effect (i.e., it is not necessary to further implement the rules into the national laws).
- **Extending the scope of crypto business models toward AML requirements:** Virtual asset transfers are subject to similar AML/CFT requirements as wire funds transfers.
- **Implementation of "Crypto Travel Rule":** Based on the FATF's modified Recommendation 16, also called the travel rule guideline, which is a guard against money laundering and other financial crimes, a "Crypto Travel Rule" is proposed. The new crypto travel rule guidance recommends that VASPs, including exchanges, banks, over-the-counter desks, hosted wallets, and other financial organizations, share certain identifying information about the recipient and receiver for cryptocurrency transactions higher than US$/€1,000 globally.
- **Prohibition of anonymous crypto wallets:** Anonymous crypto wallets are no longer allowed.
- **Prohibition of cash purchases over €10,000:** The new regulation will contain directly applicable rules, including in the areas of CDD and beneficial

ownership. It also includes establishment of an EU-wide limit of €10,000 for cash payments.

The EU Commission's AML package reflects its concern about the failure of some member states to enforce certain legislation and the delays in implementation of national laws. The goals of the AML package are to tighten cooperation, create a level playing field, and enable faster implementation of new AML Directives, without needing to fortify it in national law. The new European Union AML/CFT laws supersede local/national laws of its member states.

For this reason, regulated entities should closely follow new regulations; the time to implement them into an organization's policies, procedures, and systems could be reduced. For regulated entities across multiple EU member states, the proposed package might increase efficiency, as legislation and its AML and KYC requirements will be consistent in all states.

Another significant change is that the EU centralized system of bank account registries will greatly enhance the ability of regulated entities to validate newly onboarded customers and any counterparties in transactions. With this ability also comes great responsibility; when the information is so readily available, regulators will expect organizations to take these extra steps as a minimum.

Not long after the Sixth AML Directive came out, there was criticism regarding the loopholes still existing for crypto transactions and virtual assets. The gaps and deficiencies identified by, for example, FATF, the European Securities and Markets Authority, and the European Banking Authority, have been closed. Therefore, financial organizations that do anything with crypto must implement several additional steps to ensure they are compliant. One area of money laundering concern is the virtual assets space that is becoming increasing larger (in volume and capital size) and showing similar patterns as money laundering in the art and real estate sectors.

FATF-Style Regional Bodies

FATF-Style Regional Bodies and FATF and Associate Members

There are nine FSRBs, which have similar forms and functions to that of FATF. They are also considered FATF associate members. In setting standards, FATF depends on input from the FSRBs as much as from its own members; however, FATF remains the only standard-setting body.

The following high-level principles apply to both FATF and FSRBs:

- **Role:** Both FATF and FSRBs help jurisdictions implement FATF standards. FSRBs play an essential role in identifying and addressing whatever AML/CFT technical assistance their individual members might need. FSRBs that coordinate technical assistance for their members also offer mutual evaluation and follow-up processes.
- **Autonomy:** FATF and FSRBs are free-standing organizations that share the common goals of combating money laundering and the financing of terrorism and proliferation, as well as fostering effective AML/CFT systems.
- **Sharing common objectives and working in partnership:** Despite the autonomy of FATF and the individual FSRBs, they share a common goal in combating money laundering and the financing of terrorism and proliferation, fostering effective AML/CFT systems, and identifying and addressing threats to the financial system.
- **Reciprocity:** FATF and FSRBs operate on the basis of (mutual, joint, or common) recognition of their work, which implies that FSRBs and FATF put in place similar mechanisms for effective participation and involvement in one another's' activities.
- **Common interest:** Because FATF and FSRBs are part of a larger whole, and the success or failure of one organization can affect all organizations, protection of the FATF brand is in the common interest of both FATF and FSRBs.

Many FATF member countries are also members of the nine FSRBs:

- Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)
- Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL, formerly PC-R-EV)
- Eurasian Group (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Financial Action Task Force of Latin America (GAFILAT) (formerly known as Financial Action Task Force on Money Laundering in South America (GAFISUD)
- Inter-Governmental Action Group against Money Laundering in West Africa (GIABA)
- Middle East and North Africa Financial Action Task Force (MENAFATF)
- Task Force on Money Laundering in Central Africa (GABAC)

Asia/Pacific Group on Money Laundering (APG)

The APG, an autonomous regional AML body, was established in February 1997 at the Fourth Asia/Pacific Money Laundering Symposium in Bangkok, where it adopted its *Terms of Reference*.

The *Terms of Reference* were substantially revised in July 2012 to recognize that the FATF's revised 40 Recommendations constituted the new international standards on combating money laundering and the financing of terrorism and proliferation. The Terms included a commitment that APG members would implement these recommendations according to their specific cultural values and constitutional frameworks. It also stipulated that, to ensure a global approach, members of the APG would work closely with FATF.

The APG uses similar mechanisms as FATF to monitor and facilitate progress. The APG and FATF have reciprocal rights of attendance at each other's meetings, as well as reciprocal sharing of documents. However, the APG, as with other autonomous AML bodies, determines its own policies and

practices. It is not a precondition for participation in the APG that AML/CFT laws already be enacted.

The APG:

- Provides a focus for cooperative AML/CFT efforts in the Asia/Pacific region
- Provides a forum in which regional issues can be discussed and experiences shared, and operational cooperation among member jurisdictions is encouraged
- Facilitates the adoption and implementation by member jurisdictions of internationally accepted AML/CFT measures
- Enables regional and jurisdictional factors to be taken into account in the implementation of international AML/CFT measures
- Encourages jurisdictions to implement AML/CFT initiatives, including more effective mutual legal assistance
- Coordinates and provides practical support, when possible, to member and observer jurisdictions in the region, when requested

The APG is voluntary and cooperative in nature. The work done by the APG and its procedures are decided by mutual agreement among its members. The group was established by agreement among its members and is autonomous; it is not derived from an international treaty and is not part of any international organization.

The APG continues to grow. APG members include Afghanistan, Australia, Bangladesh, Bhutan, the Kingdom of Brunei Darussalam, Cambodia, Canada, China, the Cook Islands, Fiji, Hong Kong SAR (China), India, Indonesia, the Republic of Korea (South Korea), Japan, Lao People's Democratic Republic, Macao SAR (China), Malaysia, Maldives, The Republic of the Marshall Islands, Mongolia, Myanmar, Nauru, Nepal, New Zealand, Niue, Pakistan, Palau, Papua New Guinea, Philippines, Samoa, Singapore, Solomon Islands, Sri Lanka, Chinese Taipei, Thailand, Timor Leste, Tonga, United States of America, Vanuatu, and Vietnam.

The APG Secretariat is headquartered in Sydney, Australia.

Caribbean Financial Action Task Force (CFATF)

Given its proximity to the world's largest cocaine producers and exporters in South America's Andean region and one of the largest drug markets (the US), the Caribbean basin has long been a convenient banking center for many international criminals, including drug traffickers.

The group consists of 27 states in the Caribbean Basin and Central and South America that have agreed to implement common countermeasures to address the problems of money laundering, terrorist financing, and the financing of the WMD proliferation. It was established as the result of meetings convened in Aruba in May 1990 and Jamaica in November 1992.

The main objective of the CFATF is to achieve effective implementation of and compliance with its recommendations to prevent and control money laundering and combat the financing of terrorism. The Secretariat has been established as a mechanism to monitor and encourage progress to ensure full implementation of the Kingston Ministerial Declaration (see below).

In May 1990, representatives of Western Hemisphere countries, in particular from the Caribbean and from Central America, convened in Aruba to develop a common approach to the phenomenon of money laundering. Nineteen recommendations constituting this common approach were formulated. These recommendations, which had specific relevance to the region, complemented the FATF's 40 Recommendations.

The Jamaica Ministerial Meeting was held in Kingston in November 1992. Ministers issued the Kingston Ministerial Declaration, in which they endorsed and affirmed their governments' commitment to implement the FATF and Aruba Recommendations, the Organization of American States (OAS) Model Regulations, and the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. They also mandated the establishment of the Secretariat to coordinate the implementation of these recommendations by CFATF member countries.

The Declaration recommended laws:

- Defining money laundering based on the model laws issued by the OAS
- Concerning the seizure and forfeiture of drug proceeds and linked assets that enable the identification, tracing, and evaluation of property subject to seizure and that permit freezing orders
- Allowing judicial challenges to seizure orders by an administrative body
- Permitting forfeiture in all cases following conviction
- Permitting courts to decide that "all property obtained during a prescribed period of time by a person convicted of drug trafficking has been derived from such criminal activity"

The Caribbean nations agreed to enter into mutual assistance agreements with one another to assist in money laundering investigations. They also agreed that money laundering should be an extraditable offense subject to simplified procedures and forfeited assets should be shared among cooperating nations.

CFATF members include Anguilla, Antigua and Barbuda, Aruba, The Bahamas, Barbados, Belize, Bermuda, Cayman Islands, Curaçao, Dominica, El Salvador, Grenada, Guyana, Haiti, Jamaica, Montserrat, Saint Kitts and Nevis, Saint Lucia, Saint Maarten, Saint Vincent and the Grenadines, Suriname, Trinidad and Tobago, Turks and Caicos Islands, Venezuela, and Virgin Islands.

The CFATF monitors members' implementation of the anti-money laundering recommendations. The CFATF Secretariat is hosted by the Government of Trinidad and Tobago in the Port of Spain.

Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)

In September 1997, MONEYVAL was established by the Committee of Ministers of the Council of Europe to conduct self- and mutual-assessment exercises of the AML measures in place in Council of Europe member states that were not members of FATF. MONEYVAL became an associate member of FATF in 2006.

On October 13, 2010, the Committee of Ministers adopted the Resolution CM/Res(2010)12 on the Statute of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). The statute elevated MONEYVAL to an independent monitoring mechanism within the Council of Europe, answerable directly to the Committee of Ministers on January 1, 2011. The MONEYVAL Statute was further amended in 2013 by the Resolution CM/ Res(2013)13.

MONEYVAL members include: Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Gibraltar*, Georgia, Guernsey*, Hungary, Holy See (since April 2011)*, Isle of Man*, Israel (since January 2006)*, Jersey*, Latvia, Liechtenstein, Lithuania, Malta, Republic of Moldova, Monaco, Montenegro, Poland, Romania, Russian Federation (also a FATF member since 2003), San Marino, Serbia, Slovak Republic, Slovenia, North Macedonia, and Ukraine.

*Nonmember States of the Council of Europe.

MONEYVAL is hosted by the Council of Europe in Strasbourg, France.

Financial Action Task Force of Latin America (GAFILAT)

The Financial Action Task Force of Latin America (GAFILAT), formerly known as Financial Action Task Force on Money Laundering in South America (GAFISUD), was created in December 2000 in Cartagena de Indias, Colombia, when a memorandum of understanding was signed by government representatives from nine countries: Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, and Uruguay. Since then, several other countries have joined as full members of the task force, including Mexico (2006), Costa Rica and Panama (2010), Cuba (2012), Guatemala, Honduras, and Nicaragua (2013), and the Dominican Republic (2016).

GAFILAT was created in the style of FATF and accepts its 40 Recommendations as the international standard against money laundering and terrorist financing. It also develops enhanced recommendations to improve national policies against those crimes.

GAFILAT supports its members in the implementation of the 40 Recommendations as national legislation and the creation of a regional prevention system against money laundering and terrorist financing. The two main tools are training measures and mutual evaluations.

GAFILAT members include Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, and Uruguay.

GAFILAT has legal capacity and diplomatic status in the Argentine Republic where its Secretariat is located in Buenos Aires.

Inter-Governmental Action Group against Money Laundering in West Africa (GIABA)

GIABA was established on December 10, 1999, by a decision of the Authority of Heads of State and government of the Economic Community of West African States. In January 2006, GIABA revised its mandate to fully incorporate and properly reflect its fight against the financing of terrorism.

The objectives of GIABA are to:

- Protect the national economies and the financial and banking systems of signatory states against the proceeds of crime and the financing of terrorism
- Improve measures and intensify efforts to combat the proceeds from crime
- Strengthen cooperation among its members

GIABA members include Republic of Benin, Burkina Faso, Republic of Cape Verde, Republic of Côte d'Ivoire, Republic of The Gambia, Republic of Ghana, Guinea Bissau, Republic of Guinea, Republic of Liberia, Republic of Mali, Republic of Niger, Federal Republic of Nigeria, São Tomé and Príncipe, Republic of Senegal, Republic of Sierra Leone, and Togolese Republic.

GIABA's Secretariat is located in Dakar in Senegal, West Africa.

Middle East and North Africa Financial Action Task Force (MENAFATF)

At an inaugural ministerial meeting held in Manama, Bahrain, in November 2004, the governments of 14 countries decided to establish a FATF-style regional body for the Middle East and North Africa. The MENAFATF is voluntary in nature and was established by agreement among its members. It is not derived from an international treaty. It is independent of any other international organization and establishes its own work, rules, and procedures, which are determined by consensus of its members. It cooperates with other international bodies, notably FATF, to achieve its objectives.

Member countries of MENAFATF have agreed on the following objectives and work toward achieving them:

- Adopt and implement FATF's 40 Recommendations against money laundering and terrorist financing and proliferation, as well as the related UN Conventions and UN Security Council Resolutions as the accepted international standards in this regard, in addition to any other standards that are adopted by Arab states to enhance the fight against money laundering and the financing of terrorism and proliferation in the region.
- Implement the relevant UN treaties and agreements and UN Security Council Resolutions regarding fighting money laundering and terrorist financing.
- Cooperate to raise compliance with these standards and measures within the MENA region and work with other international organizations to raise compliance worldwide.
- Work together to identify regional money laundering and terrorist financing issues, share experiences with these problems, and develop regional solutions for dealing with them.
- Build effective arrangements and systems throughout the region to effectively fight money laundering and terrorist financing that do not contradict with the cultural values, constitutional frameworks, and legal systems of the member countries.

MENAFATF members include People's Democratic Republic of Algeria, Kingdom of Bahrain, Republic of Djibouti, Arab Republic of Egypt, Islamic Republic of Mauritania, Hashemite Kingdom of Jordan, State of Kuwait, The Lebanese Republic, State of Libya, Kingdom of Morocco, Sultanate of Oman, State of Palestine, State of Qatar, Republic of Iraq, Kingdom of Saudi Arabia, Federal Republic of Somalia, Republic of Sudan, Syrian Arab Republic, Republic of Tunisia, United Arab Emirates, and Republic of Yemen.

MENAFATF is headquartered in Manama, Bahrain.

The Eurasian Group on Combating Money Laundering and Financing Terrorism (EAG)

The Eurasian Group (EAG) was formed in October 2004 in Moscow. The EAG was created for the countries of the Eurasian region that are not included in the existing FSRBs.

The primary goals of EAG are to ensure effective interaction and cooperation at the regional level and integration of EAG member states into the international AML/CFT system in accordance with FATF's 40 Recommendations and the standards of other international organizations to which EAG member states are party.

The main tasks of EAG are:

- Assisting member states in implementing the FATF Recommendations
- Developing and conducting joint activities aimed at combating money laundering and terrorist financing
- Implementing a program of mutual evaluations of member states based on the FATF Recommendations, including assessment of the effectiveness of legislative and other measures adopted in the sphere of AML/CFT efforts
- Coordinating international cooperation and technical assistance programs with specialized international organizations, bodies, and interested states
- Analyzing money laundering and terrorist financing trends (typologies) and exchanging best practices of combating such crimes, taking into account regional specifics

The EAG members include Republic of Belarus, China, Republic of India, Republic of Kazakhstan, Kyrgyz Republic, Russian Federation, Republic of Tajikistan, Turkmenistan, and Republic of Uzbekistan.

The EAG is headquartered in Moscow, Russian Federation.

Eastern and Southern African Anti-Money Laundering Group (ESAAMLG)

The Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) is an intergovernmental body with a mandate to promote the effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other threats to the integrity of the international financial system.

Launched in Tanzania in 1999, current membership in the ESAAMLG comprises 19 countries: Angola, Botswana, Eritrea, Eswatini, Ethiopia, Kenya, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Rwanda, Seychelles, South Africa, Tanzania, Uganda, Zambia, and Zimbabwe.

The main decision-making body of the ESAAMLG is the Council of Ministers, which comprises state member ministers who manage financial matters. The group developed a Memorandum of Understanding among its member countries, in which they agreed to:

- Adopt and implement the 40 FATF Recommendations
- Apply AML measures to all serious crimes
- Implement measures to combat the financing of terrorism
- Implement any other measures contained in multilateral agreements and initiatives to which they subscribe for the prevention and control of the laundering of the proceeds of all serious crimes and the financing of terrorist activities

Region-specific projects and studies are also undertaken by the ESAAMLG. For example, a project was initiated in 2014 to obtain information, statistics, and trends related to wildlife poaching, illegal trade in wildlife products, and associated money laundering. Building from these efforts, further study of money laundering and the illegal wildlife trade has been published by FATF, including red flags such as transfers between shell companies and wildlife organizations and corruption of PEPs.

ESAAMLG is headquartered in Dar es Salaam, Tanzania.

Task Force on Money Laundering in Central Africa (GABAC)

The Task Force on Money Laundering in Central Africa known as Groupe d'Action contre le Blanchiment d'Argent en Afrique Centrale (GABAC) is a body of the Economic and Monetary Community of Central Africa. Established in 2000, its mandate is to combat money laundering and terrorist financing, assess the compliance of its members against FATF standards, provide technical assistance to its member states and facilitate international cooperation. In February 2012, GABAC became an observer organization of FATF. In October 2015, FATF recognized GABAC as an FSRB and admitted it as an Associate Member.

GABAC members include Cameroon, Central African Republic, Chad, Congo, Democratic Republic of the Congo, Equatorial Guinea, and Gabon.

GABAC is headquartered Libreville, Gabon.

Other Influencing Bodies

Organization of American States: Inter-American Drug Abuse Control Commission

In May 1992, the OAS became the first permanent international body to reach an agreement on model legislation aimed specifically at dealing with money laundering. At its annual general assembly held in Nassau, the Bahamas, the OAS unanimously approved a set of 19 articles written in statutory language that it recommended its member nations enact.

The OAS action was the culmination of a two-year effort by the Inter-American Drug Abuse Control Commission, an OAS entity that uses the acronym CICAD (Comisión Interamericana para el Control del Abuso de Drogas). In 1990, CICAD gathered a group of experts from 14 nations to craft the articles.

CICAD's role includes:

- Serving as the Western Hemisphere's policy forum on all aspects of the illegal drug trade
- Fostering multilateral cooperation on drug issues in the Americas
- Executing action programs to strengthen the capacity of member states to prevent and treat drug abuse, combat production and trafficking of illicit drugs, and deny traffickers the proceeds of crime
- Promoting drug-related research, information exchange, specialized training, and technical assistance
- Developing and recommending minimum standards for drug-related legislation, treatment, measurement of both drug consumption and the cost of drugs to society, and drug-control measures, among others
- Conducting regular multilateral evaluations of progress by member states in all aspects of illegal drug trade

CICAD's core mission is to strengthen human and institutional capabilities and harness the collective energy of member states to reduce the production, trafficking, and use of illegal drugs in the Americas. It also aims to address the health, social, and criminal repercussions of the drug trade.

Within CICAD is an Anti-Money Laundering Unit (CICAD-AMLU), which was established in 1999. The Unit focuses its efforts on providing technical assistance and training to all member states in judicial and financial measures and law enforcement. It also acts as Secretariat of CICAD's Group of Experts for the Control of Money Laundering.

Through the Group of Experts, Model Regulations are developed on money laundering offenses related to drug trafficking and other crimes, including the financing of terrorism. These regulations serve as permanent legal documents that provide a legal framework to member states. They were influenced by and are compatible with FATF's 40 Recommendations.

The entire set of Model Regulations is available at the CICAD website.

In 1999, the Inter-American Development Bank (IADB) and CICAD started a program in eight South American countries to train employees from financial organizations and financial regulatory agencies who are responsible for enforcing AML requirements. In 2001, another program was developed and conducted for judges and prosecutors within the eight countries, and, in 2002, a long-term project was begun to establish financial intelligence units in Argentina, Chile, Ecuador, Brazil, Peru, Uruguay, and Venezuela.

Egmont Group of Financial Intelligence Units

In 1995, several national FIUs began working together in an informal organization known as the Egmont Group (named for the location of the first meeting, the Egmont-Arenberg Palace in Brussels). The goal of the group is to provide a forum for FIUs around the world to improve cooperation and establish the environment needed to foster trust among countries to securely share sensitive information in the fight against money laundering and the financing of terrorism. The Egmont Group comprises several organizational groups, including the Heads of FIUs.

The support provided by the Egmont Group includes:

- Serving as the operational arm of the international AML/CFT apparatus
- Providing a platform for the secure exchange of expertise and financial intelligence to combat AML/CFT
- Expanding and systematizing cooperation in the reciprocal exchange of information
- Increasing the effectiveness of FIUs by offering training and promoting personnel exchanges to improve the expertise and capabilities of personnel employed by FIUs
- Fostering better and secure communication among FIUs through the application of technology, such as the Egmont Secure Web (ESW)
- Promoting the operational autonomy of FIUs
- Promoting the establishment of FIUs in conjunction with jurisdictions with an AML/CFT program in place or in areas with a program in the early stages of development

The Egmont Group has produced a set of governing documents to lay the foundation for the future work of the Egmont Group and contribute to greater international cooperation and information exchange among FIUs. These documents include The Egmont Charter and the Egmont Principles for Information Exchange and Operational Guidance for FIUs. The latter document is binding for members and includes several provisions, including General Framework and International Co-operation requirements. Examples of the provisions include:

- The Egmont Group fosters the development of FIUs and information exchange.
- International cooperation among FIUs should be encouraged and based upon a foundation of mutual trust.
- Information-sharing arrangements must recognize and allow room for case-by-case solutions to specific problems.
- FIUs should exchange information with foreign FIUs, regardless of their status (i.e., administrative, law enforcement, judicial, or other).

- FIUs should use the most efficient means to cooperate.
- Exchanged information should be used only for the purpose for which the information was sought or provided.

Resources provided by the Egmont Group include case studies related to money laundering, terrorist financing, fraud, and other forms of financial crimes. These case studies often consist of information compiled by reviewing cases submitted by FIUs from various jurisdictions. They can be used to assist AML professionals in identifying suspicious activity and determining whether to report these activities.

The Egmont Group undertook an initiative that resulted in the publication of "FIUs in Action: 100 Cases from the Egmont Group." According to the Egmont Group, this publication has provided invaluable assistance in identifying the components of money laundering cases. Several best practices from this analysis can benefit FIUs. Examples include: Disclosures of suspicious activity by financial organizations should continue to be made, even while an investigation is being conducted by an FIU, and additional information obtained by a financial organization's own inquiries have been shown in a number of cases to be very useful for later investigations by the authorities.

Beyond the analysis of the 100 cases, the report identifies six of the most frequently observed indicators of money laundering:

- Large-scale cash transactions
- Atypical and uneconomical fund transfers to or from a foreign jurisdiction
- Unusual business activities and transactions
- Large and/or rapid movements of funds
- Unrealistic wealth compared with client profile
- Defensive stance to questioning

Egmont membership and observer organizations continue to grow because, according to the FATF Recommendations, FIUs are expected to apply for membership.

The Wolfsberg Group

The Wolfsberg Group is an association of global banks that aims to develop financial services, industry standards, and guidance related to Know Your Customer (KYC), anti-money laundering, and counter-terrorist financing policies. The Wolfsberg Group, which has no enforcement powers, issued the guidelines to manage its members' own risks to help make sound decisions about clients and to protect their operations from criminal abuse.

The Group first came together in 2000 at the Wolfsberg castle in Switzerland, accompanied by representatives of Transparency International, to draft anti-money laundering guidelines for private banking that, when implemented, would mark an unprecedented private-sector assault on the laundering of the proceeds of corruption.

The Wolfsberg *Anti-Money Laundering Principles for Private Banking* was published in October2000 and have been routinely revised. These principles recommend controls for private banking that range from the basic, such as customer identification, to enhanced due diligence, such as heightened scrutiny of individuals who "have or have had positions of public trust."

The banks that released the Principles with Transparency International said that the Principles would "make it harder for corrupt people to deposit their ill-gotten gains in the world's banking system." The Principles state that banks must "endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate." They highlight the need to identify the beneficial owner of funds "for all accounts" when that person is someone other than the client and urge private bankers to perform due diligence on "money managers and similar intermediaries" to determine that the middlemen have a satisfactory due diligence process for their clients or a regulatory obligation to conduct such due diligence. The Principles recommend that "at least one person other than the private banker" should approve all new clients and accounts.

The Principles list several situations that require enhanced due diligence, including activities that involve:

- Politically exposed persons, such as public officials, holding or having held "senior, prominent or important public positions with substantial authority over policy, operations, or the use or allocation of government-owned resources, such as senior government officials, senior executives of

government corporations, senior politicians, important political party officials, as well as their close family and close associates."

- People residing in and/or having funds from high-risk countries, including countries "identified by credible sources as having inadequate anti-money laundering standards or representing high-risk for crime and corruption."
- People involved in types of "economic or business activities or sectors known to be susceptible to money laundering."

Clients may also require greater scrutiny as a result of:

- Information gained from monitoring their activities
- External inquiries
- Derogatory information, such as negative news reporting
- Other factors that may expose the bank to reputational risk

The Wolfsberg Principles say that banks should have written policies on the "identification of and follow-up on unusual or suspicious activities," and should include a definition of what is suspicious, as well as examples of such activity. They recommend a sufficient monitoring system that uses the private banker's knowledge of the types of activity that would be suspicious for particular clients. They also outline mechanisms that can be used to identify suspicious activity, including meetings, discussions, and in-country visits with clients and steps that should be taken when suspicious activity is detected.

The Principles also addressed:

- Reporting money laundering issues to management
- AML training
- Retention of relevant documents
- Deviations from policy
- Creation of an anti-money laundering department and an AML policy

One of the key revisions made to the Principles related to the prohibition of the use of internal nonclient accounts (sometimes referred to as concentration accounts) to keep clients from being linked to the movement of funds on their behalf. It stated that banks should forbid the use of such

internal accounts in a manner that would prevent officials from appropriately monitoring movements of client funds.

The Wolfsberg Group also issued guidelines on the suppression of the financing of terrorism, outlining the roles of financial institutions in the fight against money laundering and terrorism financing.

The Wolfsberg recommendations included:

- Providing official lists of suspected terrorists on a globally coordinated basis by relevant authorities
- Including adequate information in the lists to help institutions search customer databases efficiently
- Providing prompt feedback to institutions following circulation of the official lists
- Providing information on the manner, means, and methods used by terrorists
- Developing government guidelines for business sectors and activities identified as high-risk for terrorism financing
- Developing uniform global formats for funds transfers that assist in the detection of terrorism financing
- Protecting financial institutions with safe harbor immunity to encourage them to share information and to report to authorities
- Performing enhanced due diligence for "business relationships with remittance businesses, exchange houses, casas de cambio, bureaux de change, and money transfer agents" and other high-risk customers or those in high-risk sectors and activities "such as underground banking businesses or alternative remittance systems

In 2002, Wolfsberg issued guidelines on anti-money laundering principles for correspondent banking that outlined steps financial institutions should take to combat money laundering and terrorism financing through correspondent banking. Correspondent accounts are established by one financial institution with another financial institution to hold deposits, make payments on its behalf, and process other transactions.

The guidelines were updated in 2014 to highlight that the Principles were intended to address the risks associated with foreign correspondent

relationships, not domestic. These guidelines extend to all correspondent banking relationships an institution maintains or establishes including where the correspondent banking client is an affiliate, subsidiary, or branch of that institution. Some of the more notable recommendations are as follows.

Due diligence should be risk-based and on an ongoing basis, depending on the location, type of business, ownership, customer base, regulatory status, and AML controls of the correspondent banking client or business. It is recommended that the following elements be considered when conducting due diligence.

- Geographic risk
- Branches, subsidiaries, and affiliates of correspondent banking clients and of the institution
- Ownership and management structures of the correspondent banking client
- Client's customer base and business
- Client's products and services
- Client's regulatory status and history
- Client's anti-money laundering controls
- Client's dealings with shell banks
- Visits to the client's business
- Enhanced due diligence regarding the involvement of PEPs with the correspondent banking
  client and downstream correspondent (nested) relationships the correspondent provides
- The Principles should be part of a financial institution's larger AML program, including anti-bribery
  and corruption, fraud, and evasion of sanctions.

The Wolfsberg Group began collaborating with the Banker's Almanac in 2004 to develop the International Due Diligence Repository. Details in the Repository include copies of company bylaws, relevant licenses, extracts from commercial registers or certificates of incorporation, the most recent annual reports, information about shareholders with stakes of more than 5%,

biographies of board members and senior management, and information about each financial institution's AML policies and procedures. The initiative is a move toward standardizing due diligence information, which in itself provides a potential cost-saving in time spent seeking information from a variety of sources. Since its launch, the Banker's Almanac has added further functionality to the Repository with the inclusion of an alert service that updates users with any changes to documents or status of an institution.

The group released Monitoring, Screening and Searching Wolfsberg to provide further guidance on "the design, implementation, and ongoing maintenance of transaction monitoring frameworks for real-time screening, transaction monitoring, and retroactive searches." This document discussed the need for appropriate monitoring of transactions and customers to identify potentially unusual or suspicious activity and transactions and for reporting such to competent authorities. In particular, it covered issues related to the development of risk-based processes for monitoring, screening, and searching transactions and customers.

All of the group's publications can be found online.

The World Bank and the International Monetary Fund

The IMF and the World Bank have supported the efforts of FATF in addressing the resistance of certain nations to joining the international battle against money laundering. Since 2001, the two organizations have required countries that benefit from their financial and structural assistance programs to have effective money laundering controls.

In the joint policy paper "Enhancing Contributions to Combating Money Laundering," the two organizations detailed the steps they would take to strengthen the global assault on money laundering.

In September 2000, the IMF and World Bank started to fully integrate the battle against money laundering and other financial crimes into its surveillance exercises and programs. That month, the International Monetary and Financial Committee (IMFC), the advisors to the IMF's board of governors, issued a communiqué that said it would: (1) "prepare a joint paper with the Bank on their respective roles in combating money laundering and financial crime, and

in protecting the international financial system," and (2) "explore incorporating work on financial abuse, particularly with respect to international efforts to fight against money laundering, into its various activities, as relevant and appropriate."

In February 2001, the IMFC, along with the IMF and World Bank, issued the background paper "Financial System Abuse, Financial Crime, and Money Laundering," which explores how the organizations could "play…role[s] in protecting the integrity of the international financial system from abuse" through use of their influence to promote national anti-corruption programs.

Since then, the IMF and World Bank have become more active in combating money laundering by:

- Concentrating on money laundering over other forms of financial abuse
- Helping to strengthen financial supervision and regulation in countries
- More closely interacting with the Organisation for Economic Co-operation and Development and the Basel Committee on Banking Supervision
- Insisting on the application of international AML standards in countries that request financial assistance

In a joint meeting in April 2004, the two bodies agreed to permanently adopt their pilot program, which assesses a nation's compliance with international AML/CFT. The program put an end to FATF's practice of publicizing noncooperative countries and territories.

The World Bank and the IMF established a collaborative framework with FATF for conducting comprehensive assessments using a single global methodology of countries' compliance with FATF's 40 Recommendations. The assessments are carried out as part of the Financial Sector Assessment Program and result in a Report on the Observance of Standards and Codes (ROSC). ROSCs summarize the extent to which countries observe 12 areas and associated standards for the operational work of the IMF and World Bank. The 12 areas include: accounting, auditing, AML/CFT, banking supervision, corporate governance, data dissemination, fiscal transparency, insolvency and creditor rights, insurance supervision, monetary and financial policy transparency, payments systems, and securities regulation. The ROSCs are prepared and published at the request of the member country and summarize a countries' observance of the standards. They are used to help sharpen organizations' policy discussions with national authorities and in the

private sector, including by rating agencies, for risk-assessment purposes. Updates to the ROSCs are produced regularly, however, new reports are prepared and published every several years.

In 2002, the World Bank and the IMF developed the *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* in an effort to provide practical steps for countries implementing AML/CFT regimes in accordance with international standards. A Second Edition and Supplement on Special Recommendation IX was published in 2006. The guide describes the global problem of money laundering and terrorist financing on the development agendas of individual countries and across regions. It explains the basic elements required to build an effective AML/CFT legal and institutional framework and summarizes the role of the World Bank and IMF in those efforts.

The following table lists the important AML/CFT organizations and documents:

Group	**What is It?**
Financial Action Task Force on Money Laundering	• Intergovernmental body with member countries and member international organizations • Sets money laundering and terrorist financing standards
Basel Committee on Banking Supervision	• Established by the central bank governors of the G-10 • Promotes sound supervisory standards worldwide
European Union	• A politico-economic union of member states that are located primarily in Europe • Issues AML/CFT directives regarding legislation that member states must issue to prevent their domestic financial systems being used for money laundering and terrorist financing

Wolfsberg Group	• Association of global banks • Aims to develop standards on money laundering controls for banks
APG, CFATF, EAG, GABAC, GIABA, GAFILAT, MENAFATF, MONEYVAL, ESAALMG	• FATF-style regional bodies that have similar form and functions to those of FATF • Provide input to FATF on standards and typologies
Egmont Group	• Informal networking group of financial intelligence units
CICAD	• Commission within the Organization of American States that addresses drug-related issues, including money laundering
World Bank and International Monetary Fund	• Work together and in conjunction with FATF to encourage countries to have adequate AML laws and to review the AML laws and procedures of FATF member countries

Key US Legislative and Regulatory Initiatives

This section provides an overview of the principal elements of US laws related to money laundering and terrorism financing that affect international transactions and jurisdictions.

USA PATRIOT Act

Motivated by the terrorist attacks of September 11, 2001, and the urgent need to decipher and disable mechanisms that finance terrorism, the US Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) in October 2001 to strengthen money laundering laws and the Bank Secrecy Act (BSA) to levels unseen since the original passage of the BSA in 1970 and the Money Laundering Control Act of 1986 (Public Law 99-570), the world's first law to criminalize money laundering.

Title III of the USA PATRIOT Act (U.S. Public Law 107-56), "The International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001," contains most, although not all, of the AML-related provisions of this diverse law. The purpose of Title III is "increasing the strength of US measures to prevent, detect, and prosecute international money laundering and the financing of terrorism, to provide a national mandate for subjecting to special scrutiny foreign jurisdictions, financial organizations operating outside the United States, and classes of international transactions or types of accounts that pose particular opportunities for criminal abuse, and to ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities."

As noted in its purpose, the USA PATRIOT Act has implications for US organizations and non-US organizations that do business in the U.S. It is important to note that the regulations issued under the USA PATRIOT Act by

the US Department of the Treasury provide the detailed requirements that financial organizations must follow to comply with the provisions of the Act. These regulations are compiled in 31 Code of Federal Regulation Chapter X.

Key provisions of the USA PATRIOT Act stem from the premise that international access points to the US financial system must be controlled. Thus, the law covers a wide range of AML/CFT provisions affecting foreign businesses. These include the following:

Section 311: Special Measures for Primary Money Laundering Concerns (31 U.S.C. 5318A)

This section provides the US Department of the Treasury with the authority to apply graduated, proportionate measures against a foreign jurisdiction, foreign financial organization, type of international transaction, and type of account that the Treasury Secretary determines to be a "primary money laundering concern." By designating a country or financial organization as a primary money laundering concern, the US government can force US banks to halt many of their financial dealings with the designee. Once identified, the Treasury Department can require US financial organizations to follow any or all of the following five special measures:

1. Keep records and/or file reports on certain financial transactions, including a description of the transactions, the identities and addresses of the participants in the transactions, and the identities of the beneficial owners of the funds involved.
2. Obtain information on the beneficial ownership of any account opened or maintained in the United States by a foreign person or a foreign person's representative.
3. Identify and obtain information about customers who are permitted to use, or whose transactions are routed through, a foreign bank's payable-through account.
4. Identify and obtain information about customers permitted to use, or whose transactions are routed through, a foreign bank's correspondent account.
5. Close certain payable-through and correspondent accounts.

To ensure that all relevant factors are considered, the Treasury Secretary must consult with the Secretary of State and the Attorney General before designating a jurisdiction, organization, or specific type of transaction or account as a primary money laundering concern.

Section 311 actions are distinct from designations brought by Treasury's Office of Foreign Assets Control (OFAC), which are applied more broadly and can also trigger asset freezing obligations.

Section 312: Correspondent and Private Banking Accounts (31 U.S.C. 5318(i))

This section requires due diligence and, in certain situations, EDD for foreign correspondent accounts, which includes virtually all account relationships that organizations can have with a foreign financial organization, as well as private banking for non-US people.

The correspondent banking portions of the rule apply to US banks, credit unions, thrift organizations, trust banks, broker-dealers, futures commission merchants and introducing brokers in commodities and mutual funds, and US-based agencies and branches of foreign banks.

Foreign financial organizations covered by the rule include foreign banks, foreign branches of US banks, foreign businesses that would be considered broker-dealers, futures commission merchants, introducing brokers in commodities and mutual funds that operate in the United States, and money transmitters and currency exchangers organized in a foreign country.

The due diligence program must be "appropriate, specific, and risk-based," and, when necessary, include enhanced policies, procedures, and controls reasonably designed to identify and report suspected money laundering in a correspondent account maintained in the United States. This due diligence program must also be included in the organization's AML program.

The due diligence program must address three measures:

1. Determining whether enhanced due diligence is necessary
2. Assessing the money laundering risk presented by the correspondent account
3. Applying risk-based procedures and controls reasonably designed to detect and report suspected money laundering

Pursuant to implementing the regulation, EDD procedures must be applied to a correspondent account established for a foreign bank operating under:

- An offshore banking license
- A license issued by a foreign country designated as noncooperative by an international organization, with which designation the Treasury Secretary agrees
- A license issued by a foreign country that has been designated by the Treasury Secretary as warranting special measures pursuant to Section 311 of the USA PATRIOT Act

The EDD that must be implemented in these situations includes:

- Conducting enhanced scrutiny for possible money laundering and suspicious transactions, including:
    - Obtaining information relating to the foreign bank's AML program
    - Monitoring transactions in and out of the correspondent account in a manner reasonably designed to detect possible money laundering and suspicious activity
    - Obtaining information about the correspondent account that is being used as a payable-through account
- Determining whether the correspondent account is being used by other foreign banks that have a correspondent relationship with the foreign bank for which the correspondent account was established, and taking reasonable steps to assess and mitigate the money laundering risks associated with such accounts
- Determining, for any such foreign bank whose shares are not publicly traded, the identity of each of the owners of the foreign bank with the power to vote 10 percent or more of any class of securities of the bank and the nature and extent of the ownership interest of each such owner

The private banking portions of the rule apply to the same organizations covered by the correspondent banking provisions. Such organizations must maintain a due diligence program for private banking accounts and conduct enhanced scrutiny of private banking accounts maintained for senior foreign political figures, their immediate family members, and their close associates.

Under the rule, a private banking account is defined as (a) an account with a minimum aggregate deposit of US$1 million, (b) an account for one or more non-US people, and (c) an account that is assigned to a bank employee acting as a liaison with the non-US person.

For covered private banking accounts, US organizations must take reasonable steps to:

- Ascertain the identity of all nominal and beneficial owners of the accounts
- Ascertain whether any such owner is a senior foreign political figure
- Ascertain the source of the funds in the account and the purpose and expected use of the account
- Monitor the account to ensure its activity is consistent with the information provided regarding the source of funds and the purpose and expected use of the account, as needed, to guard against money laundering, and to report any suspected money laundering or suspicious activity

In ascertaining whether an account owner is a senior foreign political figure, the organization must take reasonable steps to determine if the person is a "current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government." The definition also covers officials of foreign political parties and government-owned commercial enterprises, as well as immediate family members and persons who are "widely and publicly known" to be close associates.

An organization that maintains accounts for these individuals must conduct enhanced scrutiny that is reasonably designed to detect if the funds "may involve the proceeds of foreign corruption," which includes any asset or property obtained "through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or … bribery or extortion."

Section 313: Prohibition on Correspondent Accounts for Foreign Shell Banks (31 U.S.C. 5318(j))

This section prohibits US banks and securities brokers and dealers from maintaining correspondent accounts for foreign, unregulated shell banks that have no physical presence. The term *physical presence* is defined as a place of business that is maintained by a foreign bank located at a fixed address (versus solely an electronic address) where it:

- Is authorized to conduct banking activities
- Employs one or more individuals on a full-time basis at that location
- Maintains operating records at that location
- Is subject to inspection by the banking authority which licensed it at that location

The term *shell bank* does not include a bank that is a regulated affiliate of a bank that maintains a physical presence.

The section also requires financial organizations to take reasonable steps to ensure that foreign banks with correspondent accounts do not themselves permit access to such accounts by foreign shell banks. Banks and securities brokers are permitted to use a certification form to comply with the rule. That process requires the foreign banks to certify at least once every three years that they are not themselves shell banks and that they do not permit shell banks access to the US correspondent account through a nested correspondent relationship.

Sections 314(a) and 314(b): Help "law enforcement identify, disrupt, and prevent terrorist acts and money laundering activities by encouraging further cooperation among law enforcement, regulators, and financial institutions to share information regarding those suspected of being involved in terrorism or money laundering."

- **Section 314(a):** FinCEN's regulations under Section 314(a) enable US federal, state, local, and foreign (European Union) law enforcement agencies, through FinCEN, to reach out to more than 43,000 points of contact at more than 22,000 financial organizations to locate accounts and transactions of persons who may be involved in terrorism or money laundering. To obtain documents from a financial organization that has

reported a match of a subject, a law enforcement agency must meet the legal standards that apply to the specific investigative tool that it chooses to use to obtain the documents.

- **Section 314(b):** 314(b) information sharing is a voluntary program. Entities that may participate in 314(b) include US financial organizations subject to an AML program requirement under FinCEN regulations, any association of such financial organizations, and unincorporated associations of financial organizations. This includes the following types of US financial organizations:
    - Banks, credit unions, and other depository institutions
    - Casinos and card clubs
    - Money services businesses
    - Brokers and dealers in securities
    - Mutual funds
    - Insurance companies
    - Futures commission merchants and introducing brokers in commodities
    - Dealers in precious metals, precious stones, and jewels
    - Operators of credit card systems
    - Loan and finance companies
    - Government-sponsored enterprises

Section 314(b) allows these financial organizations to share information with one another regarding individuals, entities, organizations, and countries for purposes of identifying and, when appropriate, reporting activities that might involve possible terrorist activity or money laundering. Section 314(b) also allows for safe harbor liability protections to share information related to activities the financial organization suspects might involve money laundering or terrorist activity, even if the financial organization or association cannot identify specific proceeds of a specified unlawful activity being laundered or the activity does not constitute a "transaction." Expanded details around Section 314(b) were included in a FinCEN Section 314(b) Fact Sheet issued in

December 2020, which rescinded previous guidance and an administrative ruling.

- **Section 319(a): Forfeiture from US correspondent account (18 U.S.C. 981(k)).** In situations in which funds have been deposited with a foreign bank, this section permits the US government to seize funds in the same amount from a correspondent bank account in the United States that has been opened and maintained for the foreign bank. The US government is not required to trace the funds, because they are deemed to have been deposited into the correspondent account. However, the owner of the funds may contest the seizure order.
- **Section 319(b): Records relating to correspondent accounts for foreign banks (31 U.S.C. 5318(k)).** This section allows the appropriate federal banking agency to require a financial organization to produce within 120 hours (5 days) records or information related to the organization's AML compliance or related to a customer of the organization or any account opened, maintained, administered, or managed in the United States by the financial organization.

  The section also allows the Treasury Secretary and the Attorney General to subpoena records of a foreign bank that maintains a correspondent account in the United States. The subpoena can request any records relating to the account, including records located outside the United States. If the foreign bank fails to comply with or fails to contest the subpoena, the Treasury Secretary or the Attorney General can order the US financial organization to close the correspondent account within 10 days of receipt of such an order.

  Additionally, the section requires foreign banks to designate a registered agent in the United States to accept service of subpoenas pursuant to this section. Furthermore, US banks and securities brokers and dealers who maintain correspondent accounts for foreign banks must keep records of the identity of the 25 percent owners of the foreign bank, unless it is publicly traded, as well as the name of the correspondent bank's registered agent in the US.

  This information is generally collected on the certification form used to comply with Section 313 and must be updated at least every three years or more frequently, if the information is no longer correct.

Anti-Money Laundering Act (AMLA) of 2020

The AMLA represents a notable development in the US AML regulatory structure first and foremost because it was the first AML-related law of substance (excluding the USA PATRIOT Act recertification) to be passed since the USA PATRIOT Act in 2001.

The law's infrastructure requires several key AML initiatives and more broadly shifts some regulatory priorities. One of the key distinctions between the USA PATRIOT Act and the AMLA is that the latter was passed as part of the National Defense Authorization Act (NDAA), which codifies the US budget and expenditures for the Department of Defense. This is notable because it is not directly promulgated by a US regulatory agency (e.g., OCC, FinCEN), and it creates a context for the language of the AMLA itself.

In addition to enhancing US AML laws (e.g., the BSA), the AMLA shifts the focus of AML compliance from a regulatory perspective to national defense. The key priorities of the AMLA are to streamline AML/CFT systems, solidify by law a risk-based approach requirement to AML/CFT compliance programs. This includes "…the establishment by financial institutions of reasonably designed risk-based programs to combat money laundering and the financing of terrorism"; creates a reporting database with uniform beneficial ownership requirements; and increases FinCEN's investigatory powers (e.g., ability to subpoena foreign bank records when those banks maintain US accounts); and requires enhanced cooperation and information sharing among financial institutions, regulators, and ultimately law enforcement-oriented agencies. The most critical language in these provisions is that, when new regulations under the AMLA are finalized, requirements should strike the proper balance between regulatory compliance and generating reporting from financial institutions (i.e., SARs and CTRs) to ensure a "high degree of usefulness to law enforcement."

One important omission is that the AMLA does not contain the words *cannabis*, *marijuana*, or *hemp*. Therefore, cannabis-related banking remains unclear. In contrast, Canada has implemented laws related to this emerging risk.

Additional expansions under the AMLA for financial organizations include:

- An expansion of civil monetary penalties to so-called “repeat” BSA violators
- New criminal offenses, such as concealing the source of funds of a monetary instrument owned or held by a senior foreign political figure
- Clawback provisions for remuneration and bonuses when the person who violated the BSA was a “partner, director, officer, or employee of a financial institution” at the time the violation of law occurred
- Prohibitions of individuals convicted of BSA violations from sitting on the board of a financial institution
- FinCEN’s authority to not only subpoena foreign financial institutions’ US account activity, but also foreign accounts
- FinCEN’s authority to demand closure of correspondent accounts and impose daily fines for the failure to do so

New requirements for the regulatory community include:

- Require FinCEN to provide reports on how SARs and CTRs are used, and which key areas make them more “useful” to law enforcement
- Encourage enhanced international cooperation between countries and their FIUs
- Provide a report on how to streamline and reduce the burden for financial organizations to report “noncomplex” cases and matters such as structuring
- Create a report with guidelines on how to derisk accounts and relationship in a safe, meaningful way that does not inhibit legitimate access to the global financial system
- Report on more or less “approved” ways to enhance AML reporting through the utilization of more advanced technology
- Publish information relating to emerging risks and trends in money laundering that can be utilized to develop and/or enhance screening typologies

The Kleptocracy Asset Recovery Rewards Act

Along with the AMLA, the NDAA also brings a legal requirement to expand the Kleptocracy Asset Recovery Rewards Act (KARRA). KARRA is effectively a whistleblower program for individuals who report on the proceeds of corruption moving through US financial organizations. This is notable because it aligns with international guidance and efforts by groups such as the FATF and the Wolfsberg Group to identify criminals in politics, as well as professional money launderers, who are referred to colloquially as "enablers." Another key provision of the AMLA is the expansion of whistleblower protection for individuals who provide "original" information related to violations of AML laws to regulators and/or prosecutors, which follows international guidance regarding whistleblower programs.

Beneficial ownership

Acknowledging the number of media events (e.g., Panama Papers, Pandora Papers) in which limited liability corporations and other corporate structures were used nearly anonymously to move vast sums of money, the AMLA aims to create a central repository for all beneficial ownership information. The structure of the Corporate Transparency Act (CTA) registry is not yet clear, but the intention is to pierce the corporate veil of anonymity for two key reasons: 1) to create transparency within those structures to find and remove potential criminals hiding behind them; and 2) to create a database for use by state and federal law enforcement entities, aimed at mitigating national security risks. The CTA utilizes a number of exemptions; however, the CTA itself and the exemptions were drafted in response to FATF criticism that the US had not policed entities created in or owned by US parties.

The CTA will ask business owners to provide, among other requirements:

- A legal form of personal identification
- Applications to form a corporate entity
- Information on the registering agent

Strategic priorities

International money laundering has long been a concern and consideration for AML/CFT risk. This section of the AMLA matches international guidance concerning:

- The screening of customers and business
- Transaction value and volume to and from high-risk jurisdictions
- Potentially high-risk third-party transactions from these jurisdictions

The AMLA also calls for the establishment of the first AML/CFT strategic priorities, which should be announced within six months of the law's passage. The strategic priorities align to FATF, the Wolfsberg Group, and other authorities' guidance on how money is laundered, for what purpose, and who is moving the funds. From a national security perspective, the strategic priorities heavily reference cryptocurrency/VC and other modalities of money laundering.

At a high level, the eight strategic priorities are:

1. **Corruption:** Noting that "corrupt actors and their financial facilitators may seek to take advantage of vulnerabilities in the US financial system to launder their assets and obscure the proceeds of crime," this objective echoes the Wolfsberg Group recommendations and guidance on the methods and means used by corrupt political figures and their enablers to launder the proceeds of corruption.
2. **Cybercrime and relevant cybersecurity and virtual currency considerations:** This strategic priority centers on cybercrime (i.e., "any illegal activity that involves a computer, another digital device, or a computer network"), but it draws parallels to traditional cybercrime (e.g., wire fraud and account takeover) and emerging cybercrime (e.g., ransomware, in which the crime takes place on a computer/system, but that system's data/information is not the actual target of the crime). This priority focuses on the misuse of cryptocurrency as a means to extort and move the proceeds of all forms of cybercrime.
3. **Foreign and domestic terrorist financing**: Consistent with FATF guidance and advisories issued by FINTRAC in Canada, this priority focuses on the misuse of the financial system for both global and domestic terrorism.

It is significant that domestic terrorism is included from an AML/CFT perspective, and this strategic priority correlates the similarities between domestic and international terrorist activity. It also references the distinctions and similarities between terrorist activity (i.e., the attack itself) and terrorist support (e.g., expenses for travel, housing, food, etc., prior to the activity itself).

4. **Fraud:** Acknowledging that crimes such as fraud "generate the bulk of illicit proceeds in the United States," this priority lists "bank, consumer, health care, securities and investment, and tax fraud" as the major sources of illicit activity within the US. There are parallels to the CTA, in that fraudulent incorporated entities are frequently utilized to launder the proceeds of fraud, although not as frequently as crimes such as tax fraud and tax evasion. This priority also draws a correlation to the "cybercrime" priority, outlining the utilization of bank and wire fraud to access accounts that are then be used to move the proceeds of cybercrime (e.g., business email compromise schemes).
5. **Transnational criminal organization activity:** Again, as a national security priority rather than simply regulatory compliance, this strategic priority uses the term "crime-terror nexus" to denote the enablement of money laundering for terrorist financing and the use of underlying crimes to raise money for terrorism. Drawing on references from the other strategic priorities, this priority specifically notes that organized crime groups might engage in or launder the proceeds of criminal activities and "maligned" activities, including "foreign election interference, attempts to stoke social unrest, and other profit-driven criminal acts" to gain the favor of individuals in seats of political power across the globe.
6. **Drug trafficking organization activity**: This strategic priority builds on international guidance concerning the use of the global financial system to place, layer, and integrate the proceeds of drug trafficking activities. It further notes that the US financial system might be used as a financial "transit" point for those proceeds, as well as their final holding place after laundering overseas. This priority also references both domestic and internationally linked sales of fentanyl and related components.

7. **Human trafficking and human smuggling**: This priority reflects the ongoing crime-terror nexus and notes that the victims of human trafficking might be used to launder money originating from the very crime by which they are being victimized. Like terrorist financing, this priority notes that often more "benign" appearing expenses, such as lodging, travel, and food, can be indicators of potential human trafficking.
8. **Proliferation financing**: Also from the national security perspective, this priority outlines both geographic and transactional risk (e.g., dual-use goods). It notes that often "gatekeepers, front or shell companies, exchange houses, or the illicit exploitation of international trade" are central to the laundering and movement of funds related to proliferation.

The Reach of the US Criminal Money Laundering and Civil Forfeiture Laws

The Money Laundering Control Act of 1986, the first criminal money laundering law of the United States, is a powerful legal weapon that may be used if the property involved in the financial transaction at issue represents the proceeds of at least one designated underlying crime—a "specified unlawful activity" (SUA). SUAs include virtually every US crime that produces economic advantage, including aircraft piracy, wire fraud, bank fraud, copyright infringement, embezzlement, export violations, illegal gambling, narcotics offenses, racketeering, and even some environmental crimes (18 USC 1956 and 1957).

This money laundering law also applies to foreign individuals and foreign financial organizations if the financial transaction occurs in whole or in part in the United States or if the foreign financial organization maintains a bank account at a US financial organization.

Although the prosecution must prove the existence of the proceeds of an SUA, it does not need to prove that the accused knew the exact source of the funds. The prosecution must prove only that the defendant knew that the funds came "from some form … of activity that constitutes a felony under state, federal, or foreign law, regardless of whether or not such activity" is an SUA (18 USC 1956(c)(1)). Courts have often ruled that willful blindness, which has been defined as "the deliberate avoidance of knowledge of the facts," is

the equivalent of actual knowledge. Willful blindness can be proven by the circumstances surrounding the transaction and the defendant's conduct.

Section 319(a) of the USA PATRIOT Act, discussed above, greatly strengthened the forfeiture powers over the funds of foreign persons and organizations. If the funds the United States pursues are deposited in a foreign bank that keeps an interbank account at a US bank, the United States may bring a case to forfeit the crime-tainted funds in the US account.

US criminal money laundering and civil forfeiture laws (Case example)

On August 5, 2021, the US Department of Justice (DOJ) announced that more than US$1.2 billion in funds misappropriated from the 1Malaysia Development Berhad (1MBD) investment fund had been returned to the people of Malaysia. From 2009 to 2015, over US$4.5 billion in funds from 1MBD was embezzled and laundered to purchase luxury real estate, fine art, hotels, fund a movie production, and pay bribes. The US District Courts in California and the District of Columbia led efforts to seize over US$1.7 billion in stolen assets.

The case exemplified the fact that all transactions that involve the US financial system are subject to US laws. Therefore, the US government can file a forfeiture complaint based on an allegation that money or property was involved in or represents the proceeds of crime.

The 1MDB investment fund was created by the government of Malaysia to promote economic development in the country through global partnerships and foreign direct investment. However, high-level 1MDB officials and their associates embezzled and laundered funds through the US, Switzerland, Singapore, and Luxemburg.

To file a civil forfeiture complaint, the US government must be able to identify the property to be seized. The US government worked with international partners to assist with tracing the use of the proceeds of the criminally derived funds. It determined that funds were used in the US to purchase luxury homes in Beverly Hills and New York and to invest in a boutique hotel in Beverly Hills and the Park Lane Hotel in Manhattan. Funds were also used to purchase luxury real estate in London, a 300-foot superyacht, and fine art by the artists Monet and Van Gogh.

Using fraudulent documents and representations, the co-conspirators laundered the funds through a series of complex transactions and shell companies with bank accounts located in the US and abroad. These transactions concealed the origin, source, and ownership of the funds, and ultimately passed through US financial institutions to then be used to acquire and invest in assets located in the US and overseas.

The Federal Bureau of Investigation (FBI) and the Internal Revenue Service's (IRS's) Criminal Investigation agency led the investigation into the misappropriated funds. Beginning in 2016, US courts and the DOJ's Money Laundering and Asset Forfeiture Section filed 41 civil forfeiture actions and seized over US$1.7 billion in stolen assets. The US DOJ received significant assistance from international government agencies and law enforcement from Malaysia, Singapore, and Luxembourg. These actions represent the largest civil forfeiture action ever initiated by the US DOJ to date.

Key takeaways

- All transactions that touch the US financial system are subject to US laws.
- The US government can file a forfeiture complaint based on an allegation that the money or property was involved in or represents the proceeds of crime.
- The US government must be able to identify the property to be seized to file a civil forfeiture complaint.
- The US government works with international partners to assist with tracing the use of proceeds of criminally derived funds; this cooperation is essential for fighting financial crime.

Office of Foreign Assets Control

In addition to these laws and regulations, financial organizations and businesses in other countries must recognize the extraterritorial reach of regulations enforced by the US Department of the Treasury Office of Foreign Assets Control (OFAC).

OFAC administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and criminals engaged in activities related to the proliferation of WMD. OFAC acts under presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under US jurisdiction. Many of its sanctions are based on United Nations and other international mandates that are multilateral in scope and involve close cooperation with allied governments.

OFAC sanction programs prohibit transactions and require the blocking of assets of persons and organizations that appear on one of several lists that OFAC issues periodically. The OFAC sanctions lists primarily include:

- **Country-based sanctions:** Sanctions brought against entire countries that prohibit nearly all types of transactions (e.g., North Korea, Iran, Cuba)
- **List-based sanctions:** Examples include the Specially Designated Nationals and Blocked Persons (SDN) list, Consolidated Sanctions list, and Foreign Sanctions Evader list, among others
- **Secondary sanctions:** sanctions directed at non-US, non-sanctioned, parties for transactions and other specific dealings with parties subject to OFAC sanctions (e.g., Iranian and Russian businesses and sectors)
- **Sectoral sanctions:** Known as “surgical or smart” sanctions in that they are applied against very focused targets to reduce subsequent collateral economic damage; for example, instead of sanctioning an entire country, sectoral sanctions target a specific sector such as energy, finance, or defense

All US people must comply with OFAC regulations, including all US citizens and permanent resident aliens, regardless of where they are located; all people and entities within the United States; and all US-incorporated entities and their

foreign branches. In the case of specific programs, such as those regarding North Korea, Syria, and Cuba, all foreign subsidiaries owned and controlled by companies also must comply. Certain programs also require foreign persons in possession of US-origin goods to comply.

OFAC recognizes that complying with sanctions can be difficult and might take time for some US parties that are newly sanctioned or currently engaging in countries, and the sanctions might adversely impact humanitarian assistance and related trade. As such, OFAC requires a license authorization to engage in a transaction that otherwise would be prohibited. There are two types of licenses: general licenses and specific licenses. A general license authorizes a particular type of transaction for a class of persons without the need to apply for a license. A specific license is a written document issued by OFAC to a specific person or entity, authorizing a specific transaction in response to a written license application.

OFAC also has the power to impose significant penalties on individuals and entities that are found to be in violation of the blocking orders within each of the sanction programs.

Office of Foreign Assets Control (Case example: US sanctions)

In 2014, OFAC reached a record US$963 million settlement with BNP Paribas SA (BNPP), Paris, France, following a US$8.9 billion penalty imposed for apparent violations of US sanctions regulations. The settlement resolved OFAC's investigation into BNPP's systemic practice of concealing, removing, omitting, and obscuring references to information about US-sanctioned parties in almost 4,000 financial transactions routed to or through US banks between 2005 and 2012. This was in apparent violation of US sanctions involving Sudan, Iran, Cuba and Burma. BNPP's methods for processing sanctions-related payments to or through the US included removing references to sanctioned parties, replacing sanctioned parties with BNPP's name or a code word, or otherwise structuring the payments in a manner that did not identify the involvement of the sanctioned parties in the transactions.

Key takeaways

- Regulated firms should have robust controls, including independent quality control and assurance, in place to detect “stripping” (i.e., the deliberate removal of key payment-related information), a common sanctions evasion technique.
- Non-US banks can be fined for noncompliance with OFAC sanctions if their transactions have a US connection, such as passing through a US bank.
- Fines and penalties associated with sanctions noncompliance can be significant and damaging to a regulated business.

Anti-Money Laundering/Countering the Financing of Terrorism Compliance Programs

Assessing AML/CFT Risk

An AML/CFT program is an essential component of a financial organization's compliance regime. The primary goal of an AML/CFT program is to protect the organization against money laundering, terrorist financing, and other financial crimes, and to ensure that the organization is in full compliance with relevant laws and regulations. For that reason, designing, structuring, and implementing these programs should be high priorities for any financial organization.

An AML/CFT program should be risk-based. Certain aspects of a financial organization's business pose greater money laundering risks than others and therefore require additional controls to mitigate those risks. Other aspects of business present a minimal risk and do not need the same level of attention.

Depending on the size of the organization, the AML function might be managed as a dedicated/standalone department, integrated into other corporate departments such as the legal department, or performed by people who have other compliance duties. Regardless of the size of the organization, the program should have an enterprise-wide view of AML/CFT efforts.

The AML/CFT program should establish minimum standards for the enterprise that are reasonably designed to comply with all applicable laws and regulations. It can be supplemented with the policies and procedures of various lines of business or legal entities that address specific areas, such as private banking, trade finance, cash handling, institutional banking, wealth management, and investigations. Compliance programs should also include corporate governance and overall management of money laundering and terrorist financing risks.

Before designing an AML/CFT program, it is imperative to understand what is required of a financial organization, its employees, and customers by the laws and regulations of all of the jurisdictions in which the organization does business and where its customers are located. The financial organization's internal policies and risk-management standards related to the business must also be taken into consideration. Anyone needing advice on the complexities of AML/CFT legislation before developing an AML/CFT program should consult a competent advisor, even if it means seeking external assistance.

This section explains what to consider when designing a compliance program; how to assess risk; how to identify, manage, document, and follow up on suspicious activities; how to know your customer and employee; how to audit your program effectively; and what you need to know about training and screening employees.

Introduction

Understanding what is legally required of an organization and its employees and customers is essential to a successful program. It is also important to understand the expectations of the relevant AML/CFT regulators and/or supervisory authorities.

FATF and its numerous member countries, such as the UK and US, urge risk-based controls. Per FATF, there are circumstances when the risk of money laundering or terrorist financing is higher, and EDD measures have to be taken.

A risk-based approach requires financial organizations to implement systems and controls that are commensurate with the specific risks of money laundering and terrorist financing they face. Therefore, assessing this risk is one of the most important steps in creating an effective AML/CFT compliance program. As money laundering risks increase, stronger controls are necessary. However, all categories of risk—whether low-, medium-, or high-level—must be identified and mitigated by the application of controls, such as verification of customer identity, customer due diligence (CDD) policies, suspicious activity monitoring, and economic sanctions screening.

The majority of governments around the world accept that the risk-based approach is preferable to a more prescriptive approach in the area of AML/CFT because it is more:

- **Flexible:** Money laundering and terrorist financing risks vary over time and across jurisdictions, customers, products, and delivery channels.
- **Effective:** Companies are better equipped than legislators to effectively assess and mitigate the specific money laundering and terrorist financing risks they face.
- **Proportionate:** A risk-based approach promotes a more practical and intelligent approach to fighting money laundering and terrorist financing than a checklist-type approach. It also allows organizations to minimize the adverse impact of AML procedures on their low-risk customers.

No financial organization can reasonably be expected to detect all wrongdoing by customers, including money laundering. But when an organization develops systems and procedures to detect, monitor, and report high-risk customers and transactions, it decreases the likelihood of being

harmed by criminals and subjected to government sanctions and penalties. The risks a financial organization faces depend on many factors, including the geographical regions (i.e., jurisdictions) involved, customer types, and the products and services offered.

When assessing risk, FATF recommends considering:

- Customer risk factors, such as nonresident customers, cash-intensive businesses, complex ownership structures, and companies with bearer shares
- Country or geographic/jurisdictional risks, such as countries with inadequate AML/CFT systems, countries subject to sanctions or embargos, countries involved with funding or supporting terrorist activities, and countries with significant levels of corruption
- Product, service, transaction, and delivery channel risk factors, such as private banking, anonymous transactions, and payments received from unknown third parties

Although it is not necessarily mandated by AML/CFT legislation in various jurisdictions, many organizations find it valuable to develop money laundering/terrorist financing (ML/TF) risk models that assess risk at the enterprise level, with the customer element providing for ML/TF risk assessments at the customer-type level (e.g., individual, company, or trust) and the specific customer level (i.e., an ML/TF risk assessment of the customer's entire relationship with the organization). Moreover, some jurisdictions also seek a separate sanctions assessment for reporting entities.

Maintaining an AML/CFT Risk Model

A risk-based approach identifies, manages, and analyzes AML/CFT risk in order to design and effectively implement appropriate controls. As such, it is critical that risk ratings accurately reflect the risks present, provide meaningful assessments that lead to practical steps to mitigate the risks, are periodically reviewed, and, when necessary, are regularly updated.

A risk-based analysis should include appropriate inherent and residual risks at the country, sectoral, legal entity, and business relationship level, among others. As a result of this analysis, the financial organization should develop a

thorough understanding of the inherent risks in its customer base, products, delivery channels, services offered (including proposed new services), and the jurisdictions within which it and its customers do business. This understanding should be based on operational, transaction and other internal information collected by the organization, as well as external sources.

In identifying all ML/TF risks, all relevant information must be taken into account. This usually requires expert input from the business lines, risk management, compliance, and legal units, together with advice from external experts, when necessary. In particular, new business products and services should be evaluated for money laundering and sanctions vulnerabilities, and appropriate controls should be implemented before launching them into the market. There is also a growing body of publicly available, helpful guidance on ML/TF risk assessments that should be taken into consideration. Such guidance is regularly published by FATF, FSRBs, regulatory agencies, other institutions such as the United Nations Office on Drugs and Crime, the IMF, the World Bank, and jurisdiction-specific information, guidance, and advisories.

Risk is dynamic and needs to be continuously managed. It should also be noted that the environment in which each organization operates is subject to continual change. Externally, the political changes of a jurisdiction and whether economic sanctions are imposed or removed can affect a country's risk rating. Internally, organizations respond to market and customer demands by merging or acquiring other companies, introducing new products and services, and implementing new delivery systems. The combination of these changes makes it critical that the ML/TF risk model is subject to regular review. In some countries, there is a legislative obligation for such reviews to be undertaken on a regular basis—usually annually or when new products, delivery channels, and customer types are introduced.

Understanding AML/CFT Risk

AML/CFT risk categories can be categorized by the following levels:

- **Prohibited:** The organization will not tolerate any dealings of any kind, given the risk. This category could include transactions with countries subject to

economic sanctions or designated as state sponsors of terrorism, such as those on the UN and OFAC lists.

- **High risk:** The risks are significant, but they are not necessarily prohibited. To mitigate the heightened risk presented, the financial organization should apply more stringent controls to reduce the ML/FT risk, such as conducting EDD and more rigorous transaction monitoring. Countries that maintain a reputation for corruption or drug trafficking are generally considered high risk. High-risk customers could include PEPs and specific types of money services businesses or cash-intensive businesses. High-risk products and services could include correspondent banking, private banking, cash services (e.g., bulk currency shipments), and international wire transfers.
- **Medium Risk:** Medium risks merit additional scrutiny, but they do not rise to the level of high risk, such as a retail business that accepts low to moderate levels of cash but is not considered cash-intensive.
- **Low Risk:** This represents the baseline risk of money laundering. Typically, low risk indicates normal, expected activity.

AML/CFT Risk

AML/CFT Risk Scoring

A risk-scoring model uses numeric values to determine the category of risk (geography, customer type, and products and services) and the overall customer risk. For example, each category could be given a score between 1 and 10, with 10 being the highest risk. The individual categories could be scored, with 1–3 being standard risk, 4–8 being medium risk, and 9–10 being high risk. Such a model is particularly helpful when analyzing product risk, because it helps determine appropriate controls for the products.

The three categories are then combined to give a composite score. A simple model would just add the totals from the categories, which would yield a score between 3 and 30. The model can be made more complex by weighting each of the factors differently, such as putting more emphasis on the type of customer, as opposed to the product or country. The model can be made even more elaborate by, for example, creating combinations of factors that will determine the overall rating. The degree of complexity is up to the organization; the more complex, the more likely the rating will reflect the customer's overall risk.

In a simple three-element model like the first one described above, care must be taken to avoid inadvertently discounting any element that is an outlier from the other elements. For example, if each element has a risk score of 3, the composite or aggregate score will be 9. However, if two of the three elements have a score of 1 and the other has a score of 7, the composite risk score is also 9. In this case, there is a need to identify how and in what manner the element scoring 7 should be mitigated. This could mean implementing a more rigorous control or introducing restrictions.

It is important to understand that, when the categories are combined, the customer's risk profile becomes clearer. For example, when you combine a product with a customer type, the combination can radically change the level of risk. For example, you have a small, foreign, private company about which you do not have much information that wants to open a checking account with online wire transfer capabilities. That customer's ability to rapidly transfer funds raises its risk level. The customer may also have higher risk ratings for geography, customer type, and products and services. Another example is a publicly listed domestic company listed on a major stock market that wants to establish an employee retirement plan. Public companies must provide extensive information to be listed on a major stock market. What is more,

retirement plan accounts are not very vulnerable to money laundering. As a result, this customer and account will pose a much lower risk than the example of the foreign private company.

The next step is to determine what thresholds to establish for each risk category. The organization should ensure that high-risk relationships do not represent too large a segment of the portfolio; this is not to say the scores should be adapted to fit the customer portfolio, rather, because high-risk customers do require more attention. In addition, if the portfolio is overly weighted toward high risk, the overall risk level in the organization could be too great to support.

Assessing AML/CFT risk is an ongoing and evolving component of maintaining a compliant AML/CFT program. It is critical to evaluate the risk-scoring model and update the risk assessment to include changes in products, services, distribution channels, customers, and jurisdiction to ensure an accurate reflection of AML/CFT risk. Although there is generally no requirement to update a risk assessment on a continuous or specified periodic basis, risk assessments should be updated before the launch of a new product, an acquisition of another financial organization, and whenever there are significant risk environment changes.

Periodically reassessing risk-rating criteria will reveal if the customers that are scored as higher risk are actually more likely to engage in potentially suspicious activity. If they are not, it may be appropriate to reassess the risk-scoring model.

Assessing the Dynamic Risk of Customers

Another critical component of a risk assessment is a process for reevaluating risks and determining when a customer risk rating should be raised or lowered. Identifying the key factors that should trigger such a reevaluation is essential to efficient allocation of limited resources.

In addition to the initial assessment of the inherent risk of a customer, it is important to consider how a customer's relationship—and risk—with the organization changes over time. Perhaps the most important consideration driving a customer's risk rating is the actual activity that the customer conducts. For example, a student checking account may start out as low-risk. But if records show that it is involved in a high number and volume of wires to

high-risk jurisdictions, indicating abnormal behavior for this customer type, the risk level for the account may need to be raised. Similarly, a potentially higher risk customer, such as an MSB or correspondent bank, might be engaging in exactly the type of activity it indicated it would conduct. This customer may not be as risky as one might think based solely on the inherent risk. As such, the low- or standard-risk student customer based solely on inherent risk might actually present more risk to the organization than the MSB, which presents a high inherent risk.

As every financial organization develops transaction history with customers, it should consider modifying the risk rating of the customer, based on:

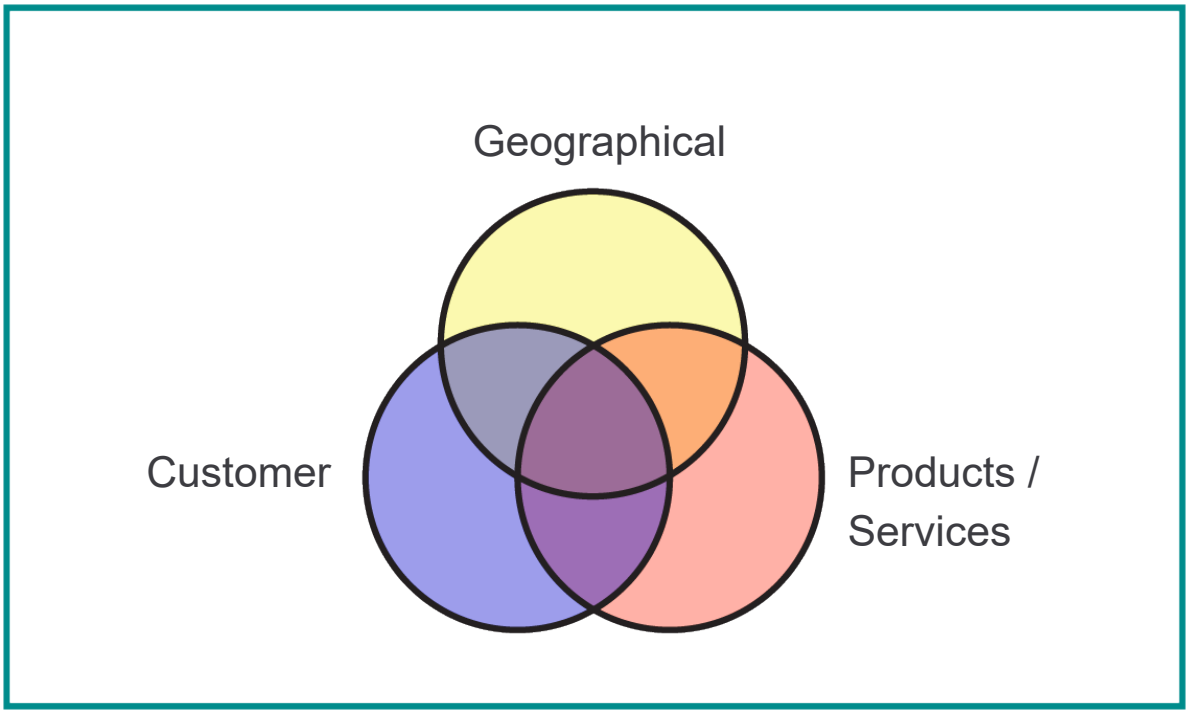
- Unusual activity, such as alerts, cases, and SAR filings
- Receipt of law enforcement inquiries, such as subpoenas
- Transactions that violate economic sanctions programs
- Other considerations, such as significant volumes of activity where it would not be expected, such as a domestic charity receiving multiple deposits (e.g., cash and electronic transfers) and then engaging in large international transactions, or businesses engaged in large volumes of cash when this would not typically be expected

A financial organization's knowledge of a customer based on its activity will better determine the actual risk presented by a customer. As noted elsewhere, higher risk customers, including those whose activity drives a higher risk rating, should be subject to EDD to mitigate the risk. This EDD might ultimately determine that the activity is not suspicious. If so, the customer record should be updated to reflect a change that explains its activity.

AML/CFT Risk Identification

The core of a risk-based approach includes the assessment of risk of a financial organization's customers, geographical locations/jurisdictions, and products and services. Following is a more in-depth explanation of these three important risk factors.

Risk types/factors



Customer type

A vital step in a risk assessment is the analysis of the users of the products and services that the organization offers. Customer types can include individuals, listed companies, private companies, joint ventures, partnerships, and financial institutions—basically anyone who wants to establish a relationship with the organization.

Customers who have a history of involvement in criminal activities receive the highest ratings. Political figures and individuals involved in political organizations also score toward the top of the scale.

Multinational public corporations tend to score lower than private companies, because there is much more publicly available information and due diligence conducted on a corporation listed on a major stock exchange. Risks are generally higher if a money launderer can hide behind corporate vehicles, such as trusts, charities, limited liability companies, and structures, for which it is difficult to identify the beneficial owners. The risk is even higher if corporations are based in countries with inadequate AML requirements or strict corporate secrecy protections.

Supervisory authorities in various countries have identified some types of customers are inherently high risk for money laundering, including:

- Banks
- Casinos
- Offshore corporations and banks located in tax/banking havens
- Embassies
- MSBs, including currency exchange houses, money remitters, and check cashers
- Virtual currency exchanges
- Car, boat, and airplane dealerships
- Used car and truck dealers and machine parts manufacturers
- Professional service providers (e.g., attorneys, accountants, investment brokers, and other third parties who act as financial liaisons for their clients)
- Travel agencies
- Broker-dealers in securities
- Jewel, gem, and precious metals dealers
- Import and export companies
- Cash-intensive businesses (e.g., restaurants, retail stores, parking)

The list above does not include all industries that could be considered high risk. It is important to note that industry alone does not determine risk. Many other types of businesses could be used to launder money, and many other factors need to be considered.

Implementing a strong screening process when onboarding a customer and throughout the duration of the relationship are key components to identifying high-risk customer types.

Geographic location/jurisdiction

A crucial step in devising a risk-scoring model involves evaluating jurisdictional risk. In what countries or jurisdictions do your individual customers reside, and what are their countries of citizenship? Where are your corporate customers headquartered, and where do they conduct the majority of their business?

There is no definitive independent system for assessing the money laundering risks of various territories and countries. Some organizations devise their own methods, while others use a vendor solution. Whichever method is chosen, it is essential that the risk-rating methodology be documented. In larger organizations, the overall risk-management strategy might require the outputs of the ML/TF risk model to be formally reviewed and endorsed by executive and senior management.

When specifically evaluating money laundering risk, the terrorism and sanctions lists published by governments and international organizations can be a useful starting point. These include lists published by the United Kingdom's Financial Conduct Authority (FCA), OFAC, FinCEN, the EU, the World Bank, the United Nations Security Council, and each local jurisdictions' regulatory and law enforcement agencies, such as Indonesia's National Counter Terrorism Agency. A risk management model should also take into account whether a country is a member of FATF or an FSRB and has AML/CFT requirements equivalent to international best practices.

Organizations might also consider the overall reputation of the countries in question. In some, cash may be a standard medium of exchange. Other countries might have politically unstable regimes and high levels of public or private sector corruption. Some might have a reputation as bank secrecy havens. Still others might be widely known to have high levels of internal drug production or to be located in drug transit regions.

How can an organization identify high-risk countries?

- The US Department of State issues an annual *International Narcotics Control Strategy Report,* which rates more than 100 countries on their money laundering controls.
- Transparency International publishes a yearly *Corruption Perceptions Index*, which rates more than 100 countries on perceived corruption.
- FATF identifies jurisdictions with weak AML/CFT regimes and issues country-specific mutual evaluation reports.
- In the US, certain domestic jurisdictions are evaluated based on whether they fall within government-identified higher risk geographic locations, such as high-intensity drug trafficking areas (HIDTAs) and high-intensity financial crime areas (HIFCAs).

Monitoring major news media is also recommended, and care should be taken that all of the country lists are monitored on a regular basis for changes.

Products and services

An important element of assessing AML/CFT risk is to review new and existing products and services that the organization or business offers to determine how they could be used to launder money or finance terrorism. The compliance officer should be an active participant in project teams that identify appropriate control frameworks for new products and systems.

What products and services does your institution offer that might be vulnerable to money laundering or terrorist financing? Internet accounts? Private banking? Money transmittal services? Stock brokerage services? Annuities? Insurance products? Offshore services? Money orders? Correspondent banking?

This risk rating, based on the type of product the customer seeks, is calculated using several product-related factors. Most notably, it depends on the likelihood that the product requested might be used for money laundering or terrorist financing. Interest-rate swaps are not likely to be used to finance terror, but securities might be vulnerable. Product scoring is not universal, because different financial organizations face varying degrees of risk.

When assessing the AML/CFT risks of products and services, consider whether they:

- Enable significant volumes of transactions to occur rapidly
- Allow the customer to engage in transactions with minimal oversight by the organization
- Afford significant levels of anonymity to the users
- Have an especially high transaction or investment value
- Allow payments to third parties
- Have unusual complexity
- Require government verification of customer eligibility

In addition, certain banking functions and products are considered high risk, including:

- Private banking
- Offshore international activity
- Deposit-taking facilities
- Wire transfer and cash-management functions
- Transactions in which the primary beneficiary is undisclosed
- Loan guarantee schemes
- Travelers checks
- Official bank checks
- Money orders
- Foreign exchange transactions
- International remittances
- Payment services such as payment processors, prepaid products, automatic clearing house
- Remote deposit capture
- Trade-financing transactions with unusual pricing features
- Payable through accounts

AML/CFT risk identification (Case example: Failure to identify high-risk activity)

In September 2020, Westpac Banking Corporation agreed to a penalty of AUD$1.3 billion for over 23 million breaches of Australia's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act. The financial regulator Australian Transaction Reports and Analysis Centre (AUSTRAC) launched legal action against Westpac in November 2019, for failing to detect and report nearly 3,000 transactions that suggested activity linked to child exploitation.

AUSTRAC accused Westpac of systemic financial crime control failures. In 2016, senior managers were alerted to the risk of suspicious payments using its low-value payment service, LitePay. Westpac did not implement controls to detect illicit activity using LitePay for two years.

According to AUSTRAC, Westpac failed to monitor customers whose activities indicated child exploitation, did not identify typologies that were indicative of child exploitation, did not apply them to transaction monitoring systems, and did not carry out appropriate customer due diligence for suspicious transactions associated with possible child exploitation.

By May 2016 Westpac had determined that the child exploitation risks relating to low-value payments to the Philippines were increasing. In response, it introduced a detection scenario to one of its payment channels that failed to detect any issues. The detection test was replaced by another in June 2018 that was an appropriate analytical tool but it was applied to only one payment channel, LitePay.

Twelve customers were identified with links to the Philippines and Southeast Asia, which are high. Eleven of them had activity patterns of frequent, low-value transactions that were consistent with child exploitation typologies. One customer had a prior conviction for child sexual exploitation, which should have triggered EDD by the bank. Six of the individuals regularly traveled to the Philippines and Southeast Asia.

AUSTRAC alleged that, if Westpac had conducted appropriate due diligence and in particular applied appropriate detection tools for child exploitation typologies, these customers would have been identified earlier. AUSTRAC found that Westpac had also failed to adequately assess high-risk

correspondent banking risks. This failure led to relationships with other banks that held nested relationships with respondents in several sanctioned and high-risk countries, including the DRC, Iraq, Libya, and Zimbabwe.

Key takeaways

- Westpac did not apply the correct typologies or monitoring tools to detect payments linked to child exploitation, even when the risks had been identified.
- Westpac did not have a consistent and clear understanding of its AML/CFT risk and how it should be managed and mitigated.
- Westpac's control failures extended to other high-risk areas such as correspondent banking.

AML/CFT Program

The Elements of an AML/CFT Program

Commonly referred to as the four pillars, the basic elements of an effective AML/CFT program are:

- A system of internal policies, procedures, and controls (first line of defense)
- A designated compliance function with a compliance officer (second line of defense)
- An ongoing employee training program
- An independent audit function to test the overall effectiveness of the AML program (third line of defense)

Although CDD requirements have traditionally been encompassed in the system of internal controls, FATF focuses particular attention on CDD as a critical means of mitigating AML/CFT risk. Under a 2016 rule, FinCEN established a fifth pillar that requires appropriate, risk-based procedures for conducting ongoing CDD, raising the prominence of this critical aspect of AML/CFT programs to its own pillar.

These procedures include:

- Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile
- Conducting ongoing monitoring to identify and report suspicious transactions
- Maintaining and updating customer information

The AML/CFT legislation in a number of countries identifies the mandatory elements of an AML/CFT program. Organizations should ensure that all such elements are addressed, based on the laws and regulations in the jurisdictions in which they operate.

A System of Internal Policies, Procedures, and Controls

The establishment and continual development of a financial organization's policies, procedures, and controls are foundational to a successful AML/CFT program. Together, these three parts define and support the entire AML/CFT program. At the same time, they serve as a blueprint that outlines how an organization fulfills its regulatory requirements. All three parts should be designed to mitigate the identified AML/CFT risks and should take into account the applicable AML/CFT laws and regulations with which the financial organization must comply. They should clearly indicate the risk appetite of the business, that is, which risks the business is prepared to accept and which it is not.

Although these controls are typically applied by the first line of defense (i.e., the employees who are responsible for onboarding customers), every employee throughout a financial organization, at all levels of the organization, must contribute to the creation, maintenance, and overall success of the AML/CFT program.

In large financial organizations, there is a critical need to adopt an enterprise-wide approach that allows for consistency in the manner in which the financial organization manages its ML/TF risk. However, there is also a need to accommodate regional and/or business line-specific requirements. For example, enterprise-wide ML/TF risk models in financial organizations that operate in multiple regions and/or countries need to reflect the local regulatory requirements. This can be achieved by having a different version of the AML/CFT program or by having country-specific addenda to the global AML/CFT program.

Internal AML/CFT policies should be established and approved by executive management and the board of directors, which sets the tone for the organization. Although the organization's policy may be a high-level statement of principles, it serves as the basis for procedures and controls that detail how lines of business will achieve compliance with laws, regulations, and the organization's AML/CFT policies.

The standard AML/CFT operating procedures should be drafted at the operational level in the financial organization. These procedures must be modified and updated, as needed, to reflect changes in laws and regulations,

products, and the organization itself. These procedures are more detailed than the corresponding AML/CFT policies; they translate policy into acceptable and workable practices. The procedures also form the basis of an important component of AML/CFT training, and the compliance monitoring programs. In addition to policies and procedures, organizations need a process to support and facilitate effective implementation of procedures, which should be reviewed and updated regularly.

Although policies and procedures provide important guidance, the AML/CFT program also relies on a variety of internal controls, including management reports and other built-in safeguards that keep the program working. These internal controls should enable the compliance department to recognize deviations from standard procedures and safety protocols. A matter as simple as requiring a corporate officer's approval or two signatures for transactions that exceed a prescribed amount could be a critical internal control element that, if ignored, seriously weakens an organization's AML/CFT program and attracts unwanted attention from supervisory authorities.

Similarly, a second review and approval of actions considered to be departures from policy could be helpful when subsequent questions arise. Other effective controls use technology, such as account opening systems that force the entry of required information, aggregation systems that detect reportable currency transactions, and automated account monitoring programs.

AML policies, procedures, and controls

An AML/CFT compliance program should be in writing and include policies, procedures, and controls that are designed to prevent, detect, and deter money laundering and terrorist financing, including how the organization will:

- Identify high-risk operations (products, services, delivery channels, customers, and geographic locations/jurisdictions).
- Periodically update its risk profile and provide for an AML/CFT compliance program tailored to manage risks.
- Inform the board of directors (or a committee of the board) and senior management of compliance initiatives, known compliance deficiencies, SARs filed, and corrective actions taken.

- Develop and maintain a system of metrics reporting that provides accurate and timely information on the status of the AML/CFT program, including statistics on key elements of the program, such as the number of transactions monitored, alerts generated, cases created, and SARs filed.
- Assign clear accountability to people for performance of duties under the AML/CFT program.
- Provide for program continuity, despite changes in management, employee composition, or structure.
- Meet all regulatory requirements and recommendations for AML/CFT compliance.
- Provide for periodic review and timely updates to implement changes in regulations, at least on an annual basis.
- Implement risk-based CDD policies, procedures, and processes.
- Provide for dual controls and segregation of duties.
- Comply with all recordkeeping requirements, including retention and retrieval of records.
- Provide sufficient controls and monitoring systems for the timely detection and reporting of potentially suspicious activity and large transaction reporting. This should also include a procedure for recording the rationale for *not* reporting activity as a result of the findings of any investigation.
- Establish clear accountability lines and responsibilities to ensure that there is appropriate and effective oversight of staff who engage in activities that might pose an AML/CFT risk.
- Establish training requirements and standards to ensure that employers are made aware of and have a working understanding of the procedures to be followed and their relevance to mitigating AML/CFT risks in their departments or areas of responsibilities.
- Clearly explain the importance of reporting suspicious activity, including describing how and to whom concerns should be raised, the role of the compliance officer, and what the “tipping off” restriction means in practice.
- Incorporate into all job descriptions and performance review processes the requirement to comply at all times with AML policies and procedures.

Noncompliance should be addressed in accordance with existing disciplinary processes.

- Develop and implement screening programs to ensure high standards when hiring employees. Implement appropriate disciplinary actions for employees who consistently fail to perform in accordance with an AML/CFT framework.
- Develop and implement quality assurance testing programs to assess the effectiveness of the AML/CFT program's implementation and execution of its requirements. This is separate from the independent audit requirement, but it serves a similar purpose—to assess the ongoing effectiveness of the program.

The level of sophistication a financial organization needs to maintain concerning its policies, procedures, and controls directly correlates to its size, structure, risk, and complexity of products, among other factors. Failure to establish, perform, follow, and maintain adequate policies, procedures, and controls can lead to severe enforcements against the organization or designated individuals involved.

Highlights of and Differences between AML/CFT Policies, Procedures, and Controls	
Policies	• Clear and simple high-level statements that are uniform across the entire organization (set the tone from the top) • Approved by executive management or the board of directors • Reflect the high-level responsibilities of the stakeholders throughout the organization

Procedures	• Translate the AML/CFT policies into an acceptable and workable practice, tasking the stakeholders with their respective responsibilities • The instructions for how an organization wants something done • Typically established at the operational (not executive) level of the financial institution • Much more detailed than AML policies • Reviewed and updated regularly
Controls	• The internal technology or tools the financial organization uses to ensure the AML/CFT program is functioning as intended and within predefined parameters • Alert compliance department to potential outliers and deviations from normal policy that may need to be reviewed • Includes management reports, automated review systems, and the utilization of multiple reviewers

A system of internal policies, procedures, and controls (Case example: Lack of overall policy control and oversight)

In October 2016, the Monetary Authority of Singapore (MAS) revoked the license of the Singapore branch of Falcon Bank Limited, due to AML/CTF failures. In 2015, an MAS investigation found that the bank's AML/CTF failings had significantly worsened following a previous inspection. One particularly serious infraction involved an individual linked to the 1Malaysia Development Berhad (1MDB) scandal and was facilitated by the actions of a former member of senior management.

MAS determined that the failings could not be rectified and ordered the closure of the branch. It also issued a fine of SGD 4.3 million, about US$3.2 million for 14 breaches of AML/CTF regulations. The Singapore branch manager was sentenced to 28 weeks in jail and personally fined SGD 128,000, about US$94,000.

MAS had first identified AML/CFT failings with Falcon Bank following an inspection in 2013. At that time, it fined the bank and ordered it to correct its AML/CTF control deficiencies in client onboarding and transaction monitoring. When MAS conducted a follow-up inspection in 2015, it found that, instead of rectifying its deficiencies, the situation had deteriorated.

Between 2012 and mid-2015, the bank's managers approved US$3.8 billion (SGD 5.2 billion) of asset transfers linked to the 1MDB fund. Despite the identification of red flags in these payments, the transactions were processed at the urging of senior management who coerced them to process the unusually large payments.

The Singapore branch manager was accused of failing to take action on more than SGD 1.3 billion or US$1 billion in payments linked to 1MDB. He was also accused of lying about his links to the alleged mastermind of the 1MDB money flows out of Malaysia. The court stated that his sentence was intended to be a deterrent to other bankers.

This case illustrates the need for an effective second line of defense. Compliance staff must provide adequate and effective challenge to the business and senior management when their actions directly or indirectly

facilitate money laundering. Regulators may impose fines and imprisonment upon staff who have willfully participated in money laundering activity.

Key takeaways

- Falcon Bank failed to remedy its AML/CTF control deficiencies, and regulators found the situation got progressively worse.
- Senior management exerted influence to facilitate transactions that were flagged as suspicious and unusually large.
- The sentencing of the Singapore branch manager was intended to be a deterrent to other bankers.

A system of internal policies, procedures, and controls (Case example: PEP risks)

In April 2017, the Hong Kong Monetary Authority (HKMA) fined the Hong Kong branch of Coutts & Co AG HKD 7 million. HKMA determined the bank failed to identify clients who were politically exposed persons (PEPs) due to a lack of effective policies and procedures. Contributing to the ineffective control framework were multiple systemic failings. These included only partial screening of customers, lack of action on screening alerts, delays in obtaining senior management approvals for customer relationships with PEPs, and undisclosed customer due diligence (CDD) failures.

Following the fine, Coutts cooperated with HKMA and adopted remedial measures to address the deficiencies.

HKMA determined that, between 2012 and 2015, Coutts failed to establish effective procedures for identifying PEPs in its customer base, including beneficial owners. This deficiency prevented PEPs from being identified by the bank, even when relevant information was publicly available.

HKMA found that Coutts had subscribed to a commercially available PEP database that generated alerts during screening, but they were not promptly addressed. HKMA found four instances of PEPs who were not identified or classified as high-risk customers, despite publicly available information.

Coutts also failed to establish effective procedures for ensuring follow-up on PEP alerts. It did not establish a management information system to oversee the approval process with senior management to continue relationships with PEPs. This violated HKMA regulatory requirements for PEP relationships to be approved. In one case, it took 34 months to obtain management approval for a PEP relationship.

Coutts limited PEP screening to new customers. There was no ongoing screening for existing customers. In addition, HKMA found deficiencies in Coutts' periodic and event-driven reviews. HKMA identified nine PEPs without management approvals, of which five had generated alerts that were not promptly addressed.

Coutts cooperated fully with the HKMA investigation. Coutts independently hired a consultant to remediate the identified customer files and review the deficiencies in their policies and procedures. These actions reduced the penalty paid by an undisclosed amount.

Key takeaways

- Effective policies and procedures for PEPs require an effective control framework based on local regulations.
- PEP screening should be conducted throughout the customer relationship. PEP policies and procedures need to explicitly and clearly direct when screening takes place. It should not be left open to interpretation.
- Controls for screening alerts and management approvals need to be consistently followed.
- Ineffective screening for PEPs and associated procedures can result in regulatory failings.

The Compliance Function

An organization's compliance function is commonly referred to as the second line of defense. It is responsible for monitoring the controls of the business, which is the first line of defense. The compliance function cannot be designed with a "one size fits all" mentality. Regardless of the structure, however, the role of the second line of defense must be established in a manner that ensures it can fulfill its role effectively.

The sophistication of the compliance function should be based on the organization's nature, size, complexity, regulatory environment, and the specific risks associated with its products, services, and customers. No two organizations will have exactly the same compliance structure, because the risks facing each organization are different, as identified in their respective risk assessments.

The Designation and Responsibilities of a Compliance Officer

In most cases, the board of directors is responsible for appointing a qualified individual as the organization's AML/CFT compliance officer. This individual is responsible for managing all aspects of the AML/CFT compliance program. This includes, but is not limited to, designing and implementing the program, making necessary changes and updates, disseminating information about the program's successes and failures to key staff members, constructing AML/CFT-related content for staff training programs, and managing the organization's adherence to applicable AML/CFT laws and regulations, including staying current on legal and regulatory developments in the field.

Communication

The ability of the compliance officer to communicate effectively, both in writing and verbally, is vital to the success of an organization's AML/CFT program. The compliance officer must also have the means to communicate at all levels of the organization—from frontline associates up to the CEO and board of directors.

It is critical for a compliance officer to be capable of articulating matters of importance to senior and executive management, particularly significant changes that could present risk to the organization, such as a sudden or substantial increase in SARs or currency transaction reports (CTRs). Other items of concern that should be escalated to management include changes to laws and regulations that might require immediate action. A compliance officer must have the skills necessary to be able to analyze and interpret these ongoing changes, determine what effect they may have on the organization, and recommend an action plan, when appropriate.

In many countries, the AML/CFT officer must also have a direct reporting line to the board or equivalent body. This unfettered access to board members allows him or her to undertake this oversight role in an effective manner. Depending upon the country, different reporting lines may exist.

Delegation of AML duties

The specific delegation of tasks and responsibilities within an AML/CFT department varies among organizations. The department could potentially be organized into subgroups with, for example, one person responsible for strategic aspects of the program and another for its operational aspects, including suspected money laundering monitoring and reporting suspicious activity.

Examples of AML/CFT subgroups include:

- **Program Management**
    - Manages and coordinates regulatory examinations
    - Performs periodic reviews and updates of the program
    - Coordinates implementation activities with the lines of business and support groups to ensure that applicable business procedures are updated to incorporate program changes
    - Monitors regulatory environment for changes to the program
    - Helps prepare training materials and provides guidance and advice on complicated AML/CFT issues not addressed by the line of business support group

- **Know Your Customer**
  - Assigns a risk code to all clients based on scoring of the CDD risk assessment
  - Performs additional due diligence on medium- and high-risk customers identified via the CDD process and customers seeking certain products and services from the financial organization
  - Provides a first line of contact for line-of-business questions on AML/CFT matters
- **Sanctions Screening**
  - Manages sanctions screening software applications and processes
  - Monitors and reconciles the data being received from the source systems
  - Fine-tunes the filter thresholds according to changes in the risk profile of the organization
  - Reviews suspected matches and reports valid matches to the appropriate regulatory authorities
- **Transaction Monitoring**
  - Manages transaction monitoring software applications
  - Monitors and reconciles the data being received from the source systems
  - Fine-tunes the filter thresholds according to changes in the risk profile of the organization
  - Participates in the design of transaction monitoring typologies and maintains the extensive documentation required

- **Financial Investigations**
    - Monitors alerts generated on customer transactions, such as those from automated systems and referrals from line-of-business staff.
    - Investigates alerts and referrals
    - Files SARs with the appropriate FIU, as required

In addition to these groups, other employees conduct AML/CFT tasks in the business lines wherever there is customer contact. For example, CDD forms are often completed by account officers and other staff members when a new account is opened, while branch personnel participate in periodic reviews of high-risk customers and might be required to provide additional information or explanation to support investigations into potentially suspicious activity. Sometimes, suspicious activity is reported to the corporate security group, which, upon determining that the activity might pose an AML/CFT risk, might refer the case to the financial investigations group.

The compliance department might also direct AML/CFT-related compliance efforts as a result of instructions from a regulatory authority or research findings. The business and the compliance function might establish risk-based quality assurance reviews and monitoring and testing activities to ensure the functions are being performed appropriately. This could include reviewing the CDD collected to ensure completeness, monitoring reports of CDD completeness or defects to ensure the systems are working as expected and performing tests to assess whether the monitoring and the business performance are satisfactorily measuring and ensuring compliance.

Compliance officer accountability

Regardless of the way an organization delegates its various AML/CFT tasks, its designated compliance officer is responsible for executing the AML/CFT program (i.e., ultimate responsibility lies with the board of directors). More and more often, various regulators are seeking enforcement actions against not only the organization, its executive management team, and board of directors for AML/CFT violations, but the compliance officer as well.

Compliance officer accountability (Case example: US bank)

In March 2020, the Financial Crimes Enforcement Network (FinCEN) of the US Department of the Treasury imposed a US$450,000 civil money penalty against Michael LaFontaine, former chief operational risk officer (CRO) at US Bank National Association (US Bank). LaFontaine was fined for his shared responsibility in failing to prevent violations of US anti-money laundering (AML) laws and regulations that occurred during his tenure.

LaFontaine held senior positions in US Bank's AML department from 2005 to 2014. According to FinCEN, his roles involved progressively more responsibility over time.

Regulators are increasingly holding senior management personally accountable for their organizations' violations of AML regulations and failure to act accordingly.

In his position as US Bank's CRO, LaFontaine reported directly to the bank's chief executive officer and communicated directly with its board of directors. His primary responsibilities included overseeing US Bank's AML compliance department and supervising the bank's chief compliance officer, AML officer, and AML staff. Due to his oversight responsibility, FinCEN determined that LaFontaine shared responsibility for US Bank's AML violations.

He failed to:

- Implement and maintain an adequate AML program
- Adequately staff the compliance program with sufficient resources to execute their regulatory expectations
- File suspicious activity reports (SARs) in a timely manner, including on transactions that potentially laundered the proceeds of crimes

FinCEN concluded that LaFontaine knew US Bank's inadequate policies, procedures, and controls would result in its failure to investigate and report suspicious and potentially illegal activity. In addition, it noted that LaFontaine

failed to exercise the responsibilities for monitoring and reporting suspicious activity by:

- Imposing upper limits on the number of alerts produced by the institution's automated transaction monitoring system
- Failing to subject Western Union money transfers to the monitoring system
- Inadequately identifying and monitoring high-risk customers in compliance with the bank secrecy act

According to FinCEN, LaFontaine was advised of the staffing issues and alert capping through internal memos. Staff claimed that significant increases in SAR volumes, law enforcement inquiries, and account closure recommendations created a situation in which AML staff resources were "stretched dangerously thin." La Fontaine failed to investigate and address the deficiencies within the department. This case illustrates the dangers of willful blindness, or deliberately ignoring and refusing to address or escalate violations.

Key takeaways

- Compliance departments should be adequately staffed to meet regulatory requirements.
- Compliance officers should escalate and act upon internal warnings and identified risks.
- Compliance officers are increasingly held personally liable for wrongdoing and may be prosecuted.
- Compliance officers should always act with integrity and do what is in the best interest of the organization.
- Compliance officers must understand their legal obligations and act in the spirit and letter of the law.

Compliance officer accountability (Case example: Personal liability)

In October 2020, the US Financial Crimes Enforcement Network (FinCEN) assessed a $60 million civil penalty against Ohio resident Larry Dean Harmon. Harmon was the founder and primary operator of the convertible virtual currency businesses Helix and Coin Ninja. Because he failed to designate a compliance officer, Harmon was the de facto compliance officer and held accountable for the organizations' compliance failures.

From 2014 through 2017, Helix and Coin Ninja operated as unregistered money services businesses (MSBs), offering anonymous convertible currency exchange services for bitcoin holders. Their customers included narcotics traffickers, counterfeiters, fraudsters, and child exploitation websites. FinCEN determined that Harmon failed to register his businesses as MSBs, implement and maintain an effective AML program, and report suspicious activity.

FinCEN determined that Harmon willfully violated Bank Secrecy Act (BSA) registration and reporting requirements. Helix and Coin Ninja provided "mixers" or "tumblers," allowing customers, for a fee, to send bitcoin to designated recipients in a manner that was designed to conceal the source or owner of the bitcoin.

Harmon knowingly obscured the nature and identity of customer transactions by:

- Designing Helix to "break the blockchain" by taking bitcoin from the user's wallet and giving the user new bitcoin from a different pool that could not be traced back to the user
- Failing to collect and verify customers' names, addresses, or identifiers on over 1.2 million transactions
- Failing to collect customer or transaction due diligence information for over US$311 million in transactions
- Deleting customer information after seven days and allowing customers to manually delete their logs

FinCEN found that Harmon actively aided cybercriminals by concealing the nature, location, source, ownership, and control of the proceeds of online drug

sales and other online illegal activities. MSBs are required to develop and maintain an AML program commensurate with the risks posed by its location, size, nature, and volume of transactions. Harmon failed to implement a system of internal controls, designate a compliance officer to oversee the BSA program, provide appropriate BSA training to personnel, and provide for an independent review of the BSA program. FinCEN identified at least 2,400 instances in which Harmon failed to file a SAR on suspicious Helix transactions.

The US Department of Justice held Harmon accountable for unlawful money laundering practices. Harmon pled guilty to criminal charges for money laundering and agreed to the forfeiture of 4,400 bitcoin as part of his plea. He may be subject to imprisonment, fines, and other restrictions.

Key takeaways

- Providers of convertible virtual currency anonymizing services are considered money transmitters under FinCEN regulations and must register as MSBs.
- MSBs are required to develop, implement, and maintain an effective AML program, including establishing a system of internal controls, designating a qualified compliance officer, implementing an appropriate training program, and providing an independent review for the program.
- FinCEN can investigate and impose civil money penalties on current and former employees of MSBs that participate in willfully violating BSA regulations.
- Individual compliance officers can be held criminally accountable for their actions, which may result in imprisonment and fines.

AML/CFT Training

Components of an effective training program

Most AML/CFT laws and regulations require financial organizations to offer as part of their formalized AML/CFT compliance programs training for relevant employees. Training is one of the most important ways to emphasize the importance of AML/CFT efforts, as well as educating employees about what to do if they encounter potential money laundering. Training also serves as an important control in the mitigation of money laundering risks to which the financial organization might be exposed.

An effective training program should not only explain the relevant AML/CFT laws and regulations, but also cover the organizations' policies and procedures used to mitigate money laundering risks. In this section, the term *training* includes both formal training courses and ongoing communications that serve to educate employees and maintain their ongoing awareness about AML/CFT requirements, such as emails, newsletters, periodic team meetings, intranet sites, and other means of sharing information. Following is an explanation of who should receive AML/CFT training, the topics that should form the basis of that training, and how, when, and where that training should be delivered.

Who to train

The first step in designing an effective AML/CFT training program is to identify the target audience. Most areas of the financial organization should receive AML/CFT training. In particular, new staff members should receive training during employee orientation or shortly thereafter. In some countries, training programs must extend beyond full- or part-time employees to include contractors, consultants, students, apprentice placements, and secondees from other branches or subsidiaries. Each segment of the staff should be trained on AML/CFT topics and issues that are relevant to their activities.

Example: Scope of Training

- **Customer-facing staff:** This is the financial organization's first line of defense; these employees need the deepest practical understanding of why AML/CFT efforts are important and what they need to do to be vigilant

against money laundering. Although a general course will often be sufficient to address the importance of AML and provide some basics, additional training on specific unit procedures related to the products and services carried out by the business line is often needed. For example, loans, credit, and loan-operations staff need training on how money launderers might misuse credit products, how the staff can recognize potential money laundering, and what the staff must do if they see it. Cash handlers often need special training because many jurisdictions have imposed additional requirements to address the increased risk posed by cash. These employees need to know how to properly handle cash transactions, especially those that trigger reporting requirements, including when to escalate concerns when a customer attempts to structure a transaction to avoid the reporting requirements. Employees who establish loans and accounts for new customers need to know applicable regulatory requirements and the organization's policies and procedures for identification and performing due diligence during the onboarding process.

- **Operations personnel:** Non-customer-facing personnel within an organization's lines of business are also included in the first line of defense and should not be overlooked in the delivery of specialized training. For example, cash vault, wire transfer, trade finance, loan underwriters, loan collections, and treasury management personnel are often in positions to recognize illegal, fraudulent, and unusual account activity. Specialized training for these individuals to recognize AML/CFT red flags and elevate unusual activity to compliance personnel should be considered.
- **AML/CFT compliance staff:** Under the direction of a designated compliance officer, the compliance staff function coordinates and monitors the organization's day-to-day AML/CFT compliance program. It is the second line of defense. Given this area's responsibility for managing the organization's adherence to AML/CFT regulations, more advanced ongoing training to stay abreast of requirements and emerging trends is important. Often, this requires attending conferences or AML/CFT-specific presentations that are more robust in nature.
- **Independent testing staff:** Independent testing personnel are the organization's third line of defense. Because this functional area independently assesses the adequacy of the AML/CFT compliance

program, these employees should receive periodic training concerning regulatory requirements, changes in regulation, money laundering methods and enforcement, and their impact on the organization.

- **Senior management and board of directors:** The board and senior management do not need the same degree of training as personnel in the first, second, and third lines of defense. Specialized training for the organization's leadership should address the importance of AML/CFT regulatory requirements, regulatory changes that impact the organization, penalties for noncompliance, personal liability, and the organization's unique risks. Without a general understanding of this information, senior management and the board cannot adequately provide for AML/CFT oversight, approve AML/CFT policies, and provide sufficient resources.

Training topics

Another factor in designing an effective AML/CFT training program is identifying the topics to be taught. This will vary according to the organization, specific products and services offered, and who is being trained.

Several basic topics should be factored into AML/CFT training, including:

- General background and history pertaining to money laundering controls, including the definitions of money laundering and terrorist financing, why criminals do it, and why stopping them is important
- Legal framework on what AML/CFT laws apply to organizations and their employees
- New and changing regulatory requirements that affect the organization
- Penalties for AML/CFT violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment
- Internal policies, such as customer identification and verification procedures and policies, including CDD, EDD, and ongoing due diligence
- Review of the internal AML/CFT and sanctions risk assessments
- Legal recordkeeping requirements
- Suspicious transaction monitoring and reporting requirements

- Currency transaction reporting requirements
- How to react when faced with a suspicious client or transaction
- How to respond to customers who want to circumvent reporting requirements
- Duties and accountability of employees
- How to maintain confidentiality with AML-related matters
- AML trends and emerging issues related to criminal activity, terrorist financing, and regulatory requirements
- Real-life money laundering schemes (preferably cases that have occurred at the organization or at similar organizations), including how the pattern of activity was first detected, its impact on the organization, and its ultimate resolution

Parties responsible for designing the training must identify which of these topics relate to the target audience.

The FCA published guidance to clarify expectations when significant AML weaknesses persist in small banks. The guidance was based on proposed examples of good practice from two thematic reviews that the FCA and its predecessor conducted. Among other issues, the FCA questioned the effectiveness of training programs, which often lacked specificity related to organizations' unique risks.

Training best practices published in the guidance included the following:

- Appropriate training tailored to the individual's specific roles. Roles lacking specific training included the following areas: offshore centers, mortgage lending, areas servicing PEPs and other high-risk clients, investment banks, and trade finance. Generic training is considered to be acceptable, provided it is supplemented with specific training with a practical application to the specific line of business or role within the organization.
- Periodic refresher training—usually annually—is important for existing employees.
- Banks should assess whether third parties and employees working in outsourced functions need to attend specific AML training.

How to train

Following are steps that trainers can take to ensure an effective AML/CFT training program:

- Identify the issues that must be communicated and decide how best to disseminate the message. Sometimes a memo or email will accomplish what is needed without formal, in-person training. Sometimes, e-learning can efficiently communicate the information. Other times, classroom training is the best option.
- Identify the audience by functional area and by level of employee/management. This can be accompanied by a brief "Why are they here?" assessment. New hires should receive training that is different from that given to veteran employees.
- Determine the needs that should be addressed. There may be issues uncovered by audits or regulatory examinations, or created by changes to systems, products, or regulations.
- Determine who can best develop and present the training program.
- Determine if "Train the Trainer" sessions are necessary, when decentralized training is involved (e.g., across large branch networks).
- Create a course abstract or curriculum that addresses course goals, objectives, and the desired results. Be sure to identify who the audience should be and how the material will be presented.
- To the extent possible, establish a training calendar that identifies the topics and frequency of each course.
- Consider whether to provide handouts. The purpose of most training handouts is to reinforce the message of the training and provide a reference tool after the training.
- Tests should be considered as a way to evaluate how well the training is understood, with a mandatory passing score. Employee scores should be retained. Similarly, if a case example is used to illustrate a point, provide a detailed discussion of the preferred course of action.

- Attention span is a factor to consider. Focus on small, easy-to-digest, and easy-to-categorize issues.
- Track employee attendance. Ask attendees to sign in and issue reminders if make-up sessions are needed. Unexcused absences might warrant disciplinary action and notation in employee personnel files.

When to train

An organization's training should be ongoing and on a regular schedule. Existing employees should at least attend an annual training session. New employees should receive appropriate training with respect to their job function and within a reasonable period after joining the organization or transferring to a new position. Situations may arise that demand an immediate session or enhanced training beyond the basic training program. For example, an emergency training session might be necessary right after an examination or audit that uncovers serious money laundering control deficiencies, a news story that names the organization, or recent regulatory action, such as a consent order, which might also prompt quick-response training. Changes in software, systems, procedures, and regulations are additional triggers for training sessions, as well as specific money laundering or other illicit financial activity risks that impact a specific business line or department.

Where to train

Some organizations have training centers that allow trainees to escape the distractions of daily work activity. Some types of training are more effective when conducted in small groups, such as the evaluation of a money laundering Case example. Role-playing exercises, which may be used to complement a prepared lecture or panel discussions, are also more effective in small groups. These training sessions can be held anywhere. Large groups can be trained using computer-based training courses, which can be designed to automatically record attendance and test attendees, with a required minimum score to demonstrate understanding of the material.

AML/CFT training (Case example)

On February 25, 2016, FinCEN and the Office of the Comptroller of the Currency (OCC) coordinated enforcement actions against Gibraltar Private Bank & Trust Company in Coral Gables, Florida, for willful AML compliance violations. The bank's substantial AML program violations, which included failure to properly train compliance staff, led to a US$2.5 million civil money penalty assessed by the OCC and a US$4 million civil money penalty assessed by FinCEN.

From 2009 to 2014, the bank's implementation of AML training was inadequate and not tailored to the needs of specific positions, departments, board members, or other personnel. For example, in 2009, senior bank officials took a basic AML course specifically designed for bank tellers, which was not appropriate, considering their functional responsibilities. In May 2013, a training assessment was undertaken by management that identified the need for significant training to adequately implement the bank's AML program. Over one year later, in 2014, regulatory authorities found that the bank had still not addressed any of the needs identified in its 2013 assessment.

Key takeaways

- It is critical that AML training be role-specific and focused on the duties and financial crime risk exposure of relevant staff.
- Senior officials and board members do not need to be trained in carrying out business functions, but they do need to understand AML requirements, penalties for noncompliance, and how to interpret risk reporting.
- Regulated firms can be heavily penalized for failing to implement adequate AML training, especially when known gaps are not addressed in a timely manner.

Independent Audit

Evaluating an AML/CFT program

Establishing an AML/CFT compliance program is not enough. The program must be monitored and evaluated. Organizations should assess their AML/CFT programs regularly to ensure their effectiveness and look for new risk factors.

The audit must be independent (i.e., performed by people not involved with the organization's AML/CFT compliance staff), and individuals conducting the audit should report directly to the board of directors or to a designated board committee composed primarily or completely of outside directors. The individuals performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable, including having knowledge and expertise of AML/CFT. Depending on the jurisdiction, an independent audit might also be referred to as an independent test or review.

The independent audit should do the following:

- Assess the overall integrity and effectiveness of the AML/CFT compliance program, including policies, procedures, and processes.
- Assess the adequacy of the AML/CFT risk assessment.
- Examine the adequacy of CDD policies, procedures, and processes, including whether they comply with regulatory requirements.
- Determine personnel adherence to the organization's AML/CFT policies, procedures, and processes.
- Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers and geographic locations/jurisdictions).
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking, and escalation procedures for lack of attendance.
- Assess compliance with applicable laws and regulations based on the jurisdictions in which the organization does business.
- Examine the integrity and accuracy of management information systems used in the AML/CFT compliance program. If applicable, this includes

assessing the adequacy of the scope of any third-party independent system validations and the qualifications of parties engaged to perform such reviews.

- Review all the aspects of any AML/CFT compliance functions that have been outsourced to third parties, including the qualifications of the personnel, contract, performance, and reputation of the company.
- Evaluate the ability of transaction monitoring software application to identify unusual activity by:
    - Reviewing policies, procedures, and processes for suspicious activity monitoring
    - Reviewing the processes for ensuring the completeness, accuracy, and timeliness of the data supplied by the source transaction processing systems
    - Evaluating the methodology for establishing and analyzing expected activity and filtering criteria
    - Evaluating the appropriateness of the monitoring reports
    - Comparing the transaction monitoring typologies with the AML/CFT risk assessment for reasonableness
- Review case management and SAR systems, including an evaluation of the research and referral of unusual transactions and a review of policies, procedures, and processes for referring unusual and suspicious activity from all business lines to the personnel responsible for investigating it.
- Assess the effectiveness of the organization's policy for reviewing accounts that generate multiple SAR filings, including account closure processes.
- Assess the adequacy of recordkeeping and record-retention processes.
- Track previously identified deficiencies and ensure management corrects them promptly.
- In coordination with the board or designated board committee, ensure that overall audit coverage and frequency are appropriate to the risk profile of the organization.
- Consider whether the board of directors was responsive to earlier audit findings.

- Determine the adequacy of the following, as they relate to the training program and materials:
    - The importance the board and senior management place on ongoing education, training, and compliance
    - Employee accountability for ensuring AML/CFT compliance, including the employee performance management process
    - Comprehensiveness of training, related to the risk assessment of each individual business line
    - Training of personnel from all applicable areas of the organization
    - Frequency of training, including the timeliness of training given to new and transferred employees
    - Coverage of internal policies, procedures, processes, and new rules and regulations
    - Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity
    - Disciplinary actions taken for noncompliance with internal policies and regulatory requirements

An effective internal audit department develops and maintains an audit risk assessment to determine audit priorities. It also develops and maintains detailed audit testing programs for every area.

All audit and regulatory recommendations for corrective action must include tracking, the target date for completion, and the personnel responsible. When a systemic violation is identified regarding a regulatory reporting requirement or other regulatory issues, the organization should perform a review back to the prior audit or examination to identify any additional issues that need to be rectified. Regular status reports on the audit and closure of findings should be provided to senior management and the board of directors. Supervisory authorities may request them.

Failure to establish and maintain a reasonably designed BSA/AML compliance program or correct a previously reported problem could result in regulatory action, such as a cease-and-desist order against an organization. Other regulatory actions include written agreements, matters requiring attention, and matters requiring board attention.

Independent audit (Case example: Apical Asset Management Pte. Ltd.)

In July 2020, the Monetary Authority of Singapore (MAS) revoked the Capital Markets Services (CMS) license of Apical Asset Management Pte. Ltd. (AAMPL) for serious breaches of MAS' AML/CFT requirements. In this case, MAS held the directors personally responsible. It reprimanded AAMPL's CEO and directors for their failure to ensure that AAMPL complied with all laws and regulations governing its operations. The failures included the lack of both an enterprise-wide risk assessment and an independent audit.

According to MAS, AAMPL committed serious breaches of MAS' AML/CFT requirements from 2013 to 2018. Specifically, AAMPL:

- Failed to conduct an enterprise-wide AML/CTF risk assessment, resulting in the failure to understand its overall vulnerability to financial crime risks and develop appropriate measures to address them
- Failed to properly assess its customers for elevated financial crime risks
- Had deficient ongoing monitoring controls and procedures
- Failed to assess the effectiveness of its AML/CFT controls by conducting independent audits

This case illustrates the need for a robust, holistic AML/CTF program that includes independent oversight to assess its effectiveness. A key component of a risk-based approach is conducting a risk assessment to identify and assess the financial crime risks an organization faces. This allows for implementation of robust controls to address these risks. MAS concluded that AAMPL did not have in place basic AML/CFT policies and procedures to manage their risks.

AML/CFT programs also need to be independently reviewed. This allows the organization to identify gaps and deficiencies to ensure continuous development and improvement. Independent testing can be done by external auditors or an internal audit function with sufficient independence from the first and second lines of defense functions. Independent internal auditors should have sufficient skills and training to conduct AML audits. They report directly to the board.

In the AAMPL case, an effective independent review would likely have identified any gaps in ongoing controls. The findings of the risk assessment would have provided the organization with the opportunity to address gaps and breaches. Instead, the regulator discovered them and revoked the company's CMS license.

Key takeaways

- A robust, holistic AML/CTF program includes independent oversight and review.
- An enterprise-wide risk assessment is needed to identify vulnerabilities and allow organizations to develop effective controls.
- Entities must assess their customers for elevated financial crime risks.
- AML/CFT policies must be in place to manage risks.

Establishing a Culture of Compliance

Embedding a culture of compliance into the overall structure of a financial organization is critical to the development and ongoing administration of an effective AML/CFT program. Typically, the ultimate responsibility for the AML/CFT compliance program rests with the organization's board of directors. The board and senior management must set the tone from the top by openly voicing their commitment to the AML/CFT program, ensuring that their commitment flows through all service areas and lines of business, and holding responsible parties accountable for compliance.

Although creating a culture of compliance may not resolve all current or future issues, an effective AML/CFT compliance program focused on identifying and controlling risks is critical to the overall success of an organization. Associates in all business units must clearly understand their commitment to supporting the compliance program by following the rules. Adopting a culture of compliance is the most effective way to prevent easily identified issues from becoming systemic problems.

An effective AML/CFT program costs money that management might be reluctant to spend. The compliance officer's challenge is to convince

management that an AML/CFT program is an indispensable expense to protect the organization and prevent legal problems and reputational harm.

As a result of FinCEN's findings of numerous financial organizations with AML/CFT compliance deficiencies, including with the roles of boards and senior management, it released an advisory in August 2014. The advisory outlined six guidelines for strengthening AML/CFT compliance culture in financial organizations:

1. Leadership must actively support and understand compliance efforts. The board's role in AML/CFT compliance consists of reviewing and approving the overall AML/CFT program and ensuring that there is ongoing oversight. Board members are not expected to become AML/CFT experts, nor are they responsible for day-to-day program management. Rather, they should be knowledgeable enough to formally approve an organization's AML/CFT compliance program and make sure it is adequately implemented and maintained by staff.

   The board's oversight role also extends to the supervisor's examination process. Examiners routinely work with the board and management before and during on-site exams to gauge the board's commitment to compliance, its understanding of the law, and its knowledge of how the organization operates. Once an exam by a supervisor or auditor is conducted, it is the board's duty to ensure that any necessary corrective action is taken. Specific duties can be delegated, but the board is responsible if problems cited by the examiner or auditor are not corrected.

   Efforts to manage and mitigate AML/CFT deficiencies and risk must not be compromised by revenue interests.

2. Compliance staff should be empowered with sufficient authority to implement an organization's AML/CFT policies. Revenue interests should not compromise or override compliance functions beyond the risk appetite of the organization. Essentially, profit should not be prioritized over compliance.

   Relevant information from the various departments within the organization must be shared with compliance staff to advance AML/CFT efforts.

3. Business units should not remain tethered within their own individual silos. Boundaries and barriers in communication should not exist within an

organization. Relevant information should be shared with the AML/CFT compliance staff.

The organization must devote adequate resources to its compliance function.

4. In addition to the requirement to designate an individual responsible for coordinating and monitoring day-to-day AML/CFT compliance under the law, leadership should provide for technology resources and appropriate AML/CFT support staff based on its risk profile.

   The compliance program must be effective. One way to ensure this is by using an independent and competent party to test the program.

5. To be effective, an AML/CFT program must include an ongoing, documented risk assessment and risk-based customer due diligence, and provide for testing by an independent, unbiased, and qualified party.

6. Leadership and staff must understand the purpose of its AML/CFT efforts and how its SAR reporting is used. Leadership and AML/CFT staff should understand the importance of filing regulatory reports. Per FinCEN, properly filed reports are used "to confront serious threats, including terrorist organizations, rough nations, weapons of mass destruction (WMD) proliferators, foreign corruption, and, increasingly, some cyber-related threats."

   Further emphasizing the need for a culture of compliance, the New York State Department of Financial Services (DFS) issued Final Rule Part 504 on June 30, 2016, requiring regulated organizations to maintain transaction monitoring and filtering programs (TMPs) reasonably designed to:

   - Monitor transactions after their execution for compliance with the BSA and AML laws and regulations, including suspicious activity reporting requirements
   - Prevent unlawful transactions with targets of economic sanctions administered by OFAC

   The Final Rule, which went into effect on January 1, 2017, also requires boards of directors or senior officer(s) of regulated organizations to make annual certifications to the DFS, confirming that they have taken all steps necessary to comply with the TMP requirements.

Although the law may seem specific to New York, numerous foreign banks are subject to the law because they operate in New York. Specifically, the law covers banks, trust companies, private bankers, savings banks and savings and loan associations chartered pursuant to the New York Banking Law, and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York. The law also applies to nonbank financial institutions with a Banking Law license, such as check cashers and money transmitters. Penalties for noncompliance are consistent with those under the Banking Law.

Importantly, the rule establishes eight minimum requirements for TMPs, in addition to specific core components of each program, which a financial organization must establish and maintain under the statute:

1. Identification of all data sources
2. Validation of the integrity, accuracy, and quality of data
3. Data extraction and loading processes to ensure a complete and accurate transfer of data
4. Governance and management oversight
5. Vendor selection process when a third-party vendor is used
6. Funding to design, implement, and maintain a program
7. Qualified personnel or outside consultant
8. Periodic training

The key to maximizing the AML/CFT unit's usefulness is to share valuable data with other areas of the organization, not just with law enforcement agencies, regulators, and senior management. As AML/CFT units build their CDD files, they might identify information other departments could use to sell products and expand profits. For example, marketing departments that better understand the activity of certain retail and business customers can more effectively identify opportunities to market additional products and deepen the overall customer relationship.

Before releasing customer information, it is important to review applicable privacy laws (e.g., Europe's General Data Protection Regulations [GDPR]) and the firm's privacy policy to understand any limitations. In principle, AML laws

and data privacy laws should not be mutually exclusive or contradictory. There are usually no regulatory limits on sharing customer information with other internal departments within the same legal entity; however, there might be limitations on sharing with other affiliated companies within a larger organization. Some organizations restrict the sharing of customer information outside the organization, and customers may opt-out of the right for the organization to provide their information to third-party companies.

Compliance staff should be sufficiently independent of the lines of business they support so that potential conflicts of interest are minimized; they should not be provided incentives based on the profitability of those business lines. This does not mean that compliance staff should not receive bonuses; however, incentives should not be structured in a way that might create a conflict of interest.

Although the compliance staff may be situated within the line of business and report to line management, they should have the ability to escalate issues without fear of recrimination to a compliance or risk-management function outside the line of business. A close working relationship of compliance staff with the line of business is crucial to a successful execution of the AML/CFT program. Ultimately, the compliance staff should be seen as trusted advisors so that the business line staff will come to the compliance staff when they have questions and will follow the advice provided.

Culture of compliance (Case example: Poor management oversight)

In July 2020, the Monetary Authority of Singapore (MAS) revoked the capital markets services license of Apical Asset Management (AAM). The MAS cited inadequate AML/CFT policies and procedures, deficient customer risk assessments, and severe deficiencies in the control framework. It also faulted senior management for not ensuring that asset managers followed relevant financial crime rules and regulations. The asset managers had also failed to undertake an enterprise-wide risk assessment (EWRA), despite an MAS requirement that the assessment be completed at least every two years. Additionally, there was no independent audit of AAM's controls to test their effectiveness.

In this case, the CEO and director of AAM were specifically reprimanded for their failings, given their ultimate responsibility for the organization's compliance with MAS requirements.

MAS identified several significant failings in AAM's financial crime controls between 2013 and 2018. These deficiencies included the lack of basic AML/CFT controls, which put the organization at risk of receiving illicit funds. MAS determined that this risk had been exacerbated by the nature of AAM's customer base, including multiple customers with complex ownership structures.

AAM did not adequately assess its customers' risks, and its ongoing monitoring controls were ineffective. In one instance, a fund related to a PEP was not subject to enhanced monitoring over an extended period of time. Increasing the risk, there was no independent audit of AAM's control framework to test whether the financial crime controls were operating effectively.

Senior management must set the overall tone and develop a culture of compliance throughout an organization. They must allocate sufficient resources to the compliance team to enable it to function as an effective second line of defense. Although senior managers do not need to review every aspect of the compliance program, they must exercise sufficient oversight of the compliance structure and processes. They also need to review key performance indicators of how well the control framework is functioning.

AAM's senior management did not exercise their oversight functions to ensure the organization complied with all applicable financial crime laws and regulations. They did not conduct an EWRA, which MAS considers essential for an entity to identify its financial crime risks and determine the appropriate controls to mitigate them.

Key takeaways

- AAM had inadequate AML/CFT policies and procedures and client risk assessments.
- There were severe deficiencies in the control framework and no independent audit.
- Accountability begins and ends with the senior management of an organization.
- Failures by senior management to discharge their duties can result in systemic failings across an organization.
- Failure to meet regulatory requirements can result in the loss of a business license.

Know Your Customer

Customer Due Diligence

A sound CDD program is one of the most effective ways to prevent money laundering and other financial crimes. Knowledge is what the entire AML/CFT compliance program is built upon. The more an organization knows about its customers, the greater chance of preventing money laundering abuses. In fact, the US Federal Financial Institutions Examination Council (FFIEC) described the cornerstone of a strong AML compliance program as the adoption and implementation of comprehensive CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. In most cases, the typical and basic CDD collected is sufficient. In other cases, further due diligence is required and could be extensive. The organization's CDD program must have a process in place to consider each level of due diligence that might be necessary, as well as who is responsible for collecting, verifying, and keeping the information updated and accurate.

According to the FFIEC, the objective of CDD should be to enable the financial organization to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes assist the financial organization in determining when transactions are potentially suspicious.

CDD is Recommendation 10 in FATF's updated Recommendations. FATF recommends that financial organizations be required to undertake CDD measures when:

- Establishing business relationships
- Carrying out occasional transactions under certain circumstances
- There is a suspicion of money laundering or terrorist financing
- The financial organization has doubts about the veracity or adequacy of previously obtained customer identification data

Main Elements of a Customer Due Diligence Program

FATF recommends that organizations incorporate the following four measures into their CDD programs:

1. Identify the customer and verify the customer's identity using reliable, independent source documents, data, and information.
2. Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner.
3. Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.
4. Conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the organization's knowledge of the customer, their business, risk profile, and, when necessary, the source of funds.

A sound CDD program should include the seven elements outlined in the table below.

Elements of a Sound CDD Program	
Element	Description
Customer identification	Obtain full identification of customer and business entities, including source of funds and wealth, when appropriate. The organization should ensure there is a process in place to update and maintain current customer information.

Profiles	Develop transaction and activity profiles for each customer. Profiles should contain sufficient information to allow for reviews of anticipated versus actual account activity and to otherwise enable the organization to identify suspicious activity based on comparing the activity with what it knows about the customer.
Customer acceptance	Define and accept the customer in the context of their use of specific products and services, which may differ among customers and geographic markets.
Risk rating	Assess and grade risks presented by the customer's account relationship. Numerous factors should be considered when determining risk, including customer type, products and services, transactional activity, and geographic locations. No single factor should be used to determine risk, with the exception of a factor that constitutes an impermissible activity, such as violating economic sanctions or illegal activity.
Monitoring	Monitor accounts and transactions based on the risks presented.
Investigation	Investigate and examine unusual customer and account activity, which should be consistent with the anticipated activity for each customer, based on occupation or type of business.
Documentation	Document findings as evidence or to provide a record of actions performed. "If it is not documented, it never happened."

Enhanced Due Diligence

In its interpretive note to Recommendation 10, FATF acknowledges that there are circumstances in which the risk of money laundering or terrorist financing is higher and EDD measures must be taken. Risk factors that warrant EDD measures include:

Customer risk factors

- Unusual circumstances regarding how the business relationship is conducted, such as significant, unexplained geographic distance between the financial organization and the customer
- Nonresident customers
- Legal persons or arrangements that are personal asset-holding vehicles
- Companies that have nominee shareholders or shares in bearer form
- Cash-intensive businesses
- Unusual or excessively complex appearance of the ownership structure of the company, given the nature of the company's business

Country or geographic risk factors

- Countries identified by credible sources, such as FATF's mutual evaluations and detailed assessment reports, as not having adequate AML/CFT systems
- Countries subject to sanctions, embargoes, and similar measures issued by, for example, the United Nations
- Countries identified by credible sources as having significant levels of drug trafficking, corruption, financial crimes, or other criminal activity
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within them
- Countries that share a common border and are known to have physical cross-border transactional activity
- Geographic areas identified as having a higher risk of money laundering or financial crimes, such HIFCAs and HIDTAs in the United States

Product, service, transaction, and delivery channel risk factors

- Private banking
- Anonymous transactions (which might include cash)
- Non-face-to-face business relationships and transactions
- Payment received from unknown or unassociated third parties

The Basel Committee, in its *Sound Management of Risks Related to Money Laundering and Terrorist Financing* states that EDD may be essential for individuals planning to maintain a large account balance and conduct regular, cross-border wire transfers and individuals who are PEPs.

Enhanced Due Diligence for High-Risk Customers

Customers that pose higher money laundering and terrorist financing risks present increased exposure to financial organizations. High-risk customers and their transactions should be reviewed even more closely at account opening and more frequently (e.g., annually) during their account relationships.

A financial organization should consider obtaining additional information from high-risk customers, such as:

- Source of funds and wealth
- Identifying information on individuals with control over the account, such as signatories and guarantors
- Occupation or type of business
- Financial statements
- Banking references
- Domicile
- Proximity of the customer's residence, place of employment, and place of business to the bank

- Description of the customer's primary trade area and whether international transactions are expected to be routine
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers
- Explanations for changes in account activity

For high-risk customers, both Wolfsberg's Correspondent Banking Principles and FATF recommend obtaining the approval of senior management to commence or continue the business relationship, as well as requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Account Opening, Customer Identification, and Verification

A sound CDD program should have reliable customer identification and account-opening procedures that allow the financial organization to determine the true identity of customers. Organizations should also set identification standards tailored to the risk posed by specific customers. In some countries, authorities have issued specific regulations and laws that detail what organizations are required to do regarding customer identification.

The Basel Committee's *Sound Management of Risks Related to Money Laundering and Financing of Terrorism* states that a bank should establish a systematic procedure for identifying and verifying its customers and, when applicable, any person acting on their behalf and any beneficial owners. Although the committee focused on banks, its recommendations can apply to any financial organization that opens accounts.

A bank should not establish a banking relationship or carry out any transactions until the identity of the customer has been satisfactorily established and verified in accordance with FATF Recommendation 10. The identity of customers, beneficial owners, and persons acting on their behalf, should be verified using reliable, independent source documents, data, and information. Regulated organizations should recognize that some identification documents are more vulnerable to fraud than others. For those that are most susceptible to fraud, or when there is uncertainty concerning

the validity of the documents presented, the verification requirements should be enhanced, and the information provided by the customer should be verified through additional inquiries and other sources of information.

The Basel Committee provided guidelines for account opening and customer identification in *Annex IV General Guide to Account Opening*. This document does not address every eventuality; rather, it focuses on some methods banks can use to develop effective customer identification and verification programs.

The annex divides customers into two groups—natural people seeking to open an account and legal people and legal arrangements—and addresses what types of information should be collected and verified for each.

Each new customer who is a natural person that opens a personal account should be asked for the following information:

- Legal name (first and last) and any other names used (e.g., maiden name, former legal name, or alias)
- Complete residential address and, on the basis of risk, also the business address or post office number
- Landline or mobile telephone numbers and email address
- Date and place of birth
- Gender
- Nationality and residency status
- Occupation, position held, and name of employer
- An official personal identification number or other unique identifier
- Type of account and nature of the banking relationship
- Signature

The organization should verify this information using reliable, independently sourced documents and data.

Documentary customer verification procedures include:

- Confirming the identity from an unexpired official document that bears a photograph of the customer
- Confirming the date and place of birth from an official document

- Confirming the validity of the official documentation through certification by an authorized person
- Confirming the residential address

Nondocumentary customer verification procedures include:

- Contacting the customer by telephone or letter to confirm the information supplied after an account has been opened
- Checking references provided by other financial organizations
- Using an independent information verification process, such as by accessing public registers, private databases, and other reliable independent sources

In some jurisdictions, other documents of an equivalent nature may be offered as satisfactory evidence of a customer's identity.

Particular attention needs to be focused on customers who are assessed as having high-risk profiles.

Additional sources of information and enhanced verification procedures may include:

- Confirming an individual's residential address on the basis of official papers, a credit reference agency search, or through home visits
- Checking prior bank reference (including banking group reference) and contacting the bank regarding the customer
- Verifying income sources, funds, and wealth identified through appropriate measures
- Verifying employment and public positions held
- Obtaining a personal reference from an existing customer of the financial organization

If national law allows for non-face-to-face account opening, financial organizations should take into account the specific risks associated with this method. Customer identification and verification procedures should be equally effective and similar to those implemented for face-to-face interviews. As part of broader CDD measures, the organization should

consider, on a risk-sensitive basis, whether the information regarding sources of wealth, funds, and destination of funds should be corroborated.

For legal people that are not natural people or legal arrangements, the following information should be obtained:

- Name, legal form status, and proof of incorporation of the legal person
- Permanent address of the principal place of the legal person's activities
- Mailing and registered address of legal person
- Identity of natural people who are authorized to operate the account; in the absence of an authorized person, the identity of the relevant person who is the senior managing official
- Contact telephone numbers
- Official identification number
- Powers that regulate and bind the legal person
- Identity of the beneficial owners
- Nature and purpose of activities of the legal entity and its legitimacy
- Financial situation of the entity
- Expected use of the account—amount, number, type, purpose, and frequency of the transactions expected—on the basis of risk; sources of funds paid into the account; and destination of funds passing through the account

The bank should verify the identity of the customer using reliable, independent source documents, data, or information.

Documentary verification methods include:

- Obtaining a copy of the certificate of incorporation, memorandum and articles of association, partnership agreement, or any other document certifying the existence of the entity
- For established corporate entities, reviewing a copy of financial statements (audited, if available)

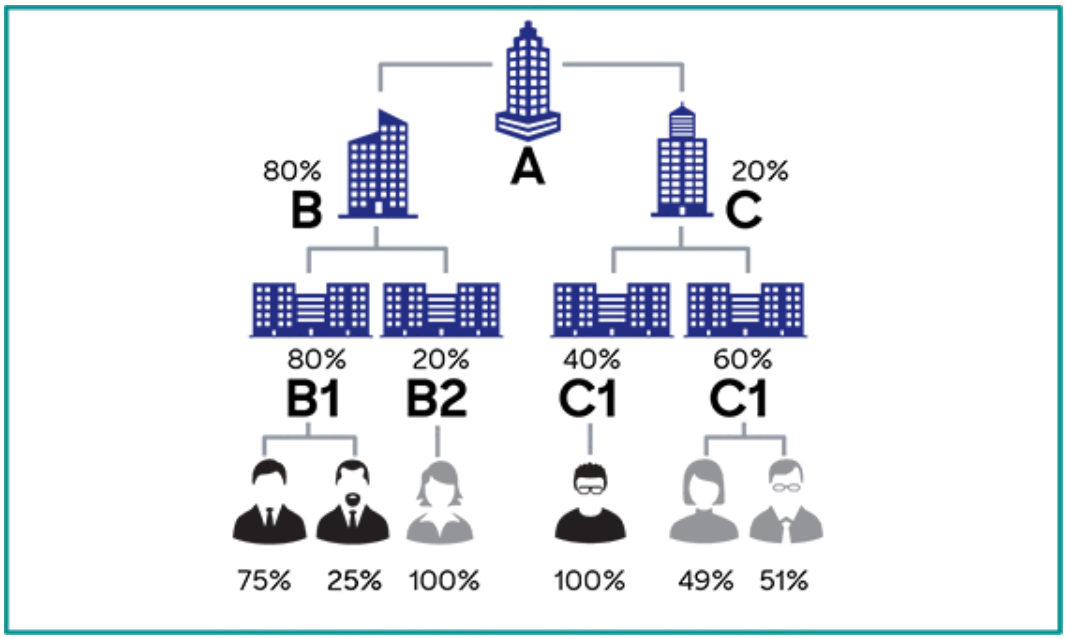
Nondocumentary verification methods include:

- Undertaking a company search and/or other commercial inquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved or terminated
- Using an independent information verification process, such as by accessing public corporate registers, private databases, or other reliable independent sources (e.g., lawyers and accountants)
- Validating the legal entity identifier and associated data in the public access service
- Obtaining prior bank references
- Visiting the corporate entity, when practical
- Contacting the corporate entity by telephone, mail, or email

The organization should verify that any person purporting to act on behalf of the legal person is so authorized. If so, the organization should verify the identity of that person as well. They should also take reasonable steps to verify the identity of the beneficial owners. However, the exact account-opening procedures and customer acceptance policies will depend on the type of customer, risk, and local regulations.

After collecting and verifying customer information, the organization needs to implement processes to maintain updated and accurate customer information, as well as determine who is responsible for these processes, such as the relationship manager. Outdated and inaccurate information can affect key processes, such as EDD reviews, watchlist screening, and transaction monitoring.

Beneficial ownership structure example



ID&V (Case example: Danske Bank)

In 2007, Danske Bank acquired Finnish Sampo Bank and its Estonian branch. Between 2007 and 2015, the Estonian branch expanded its nonresident portfolio. Nearly all of its customers were offshore and shell companies, many with links to high-risk countries. The parent bank was unaware of the structure of the client portfolio, because there was no integrated client list, and it relied on the information provided by the Estonian branch. Over an eight-year period, approximately US$200 billion in transactions were processed by the Estonian branch, most of which later were deemed suspicious by regulators. The Estonian branch was closed in 2019 by order of the Estonian Financial Supervisory Authority (FSA).

Danske Bank violated AML/CFT regulations in multiple areas. After the acquisition of Sampo Bank, the Estonian branch was never integrated into the group's IT compliance infrastructure. The group-wide AML and KYC policies and procedures were not shared with the Estonian branch. This omission led to a fragmented and inconsistent KYC implementation within Danske Bank.

Investigators discovered that the Estonian branch employees' understanding of money laundering risks was limited, and there were significant deficiencies

in their AML controls. The Estonian branch performed limited KYC, focused solely on credit risk. They did not identify money laundering, terrorist financing, sanctions, or tax evasion risks and the KYC, AML, and risk management units were not integrated with the group.

Danske Bank failed its legal obligations and underestimated the risk of its customer portfolio. It also failed to apply EDD measures consistent with laws and regulations and its group-wide requirements. For example, it did not screen incoming payments for sanctions, performed no PEP screening, and failed to respond to suspicious customers and transactions. The suspicious criminal activity was escalated to Danske Bank's senior management but an internal audit conducted by the bank did not find suspected money laundering and no further action was taken by the bank.

AML officers must integrate their organization's AML/CFT and KYC frameworks across their companies, including branches and subsidiaries. They should conduct a thorough risk assessment and ensure that appropriate customer risk-rating methodology is implemented. Policies and procedures must be implemented organization-wide to ensure AML/CFT and KYC processes are robust and consistent, including the application of EDD, when appropriate. IT systems that screen customers and identify suspicious activity need to be integrated to support processes and risk management, including a holistic risk view.

Key takeaways

- Organizations must integrate the AML/CTF and KYC frameworks of new acquisitions immediately with a thorough risk assessment.
- Organizations should apply AML/CTF and KYC policies and procedures organization-wide.
- Organizations need to have a consistent customer risk-rating methodology.
- Organizations need to have robust and consistent KYC processes, including EDD.
- Dedicated AML teams should operate independent from the business.
- A strong AML culture should be embedded across the organization with clear oversight and direction from senior management.

Consolidated Customer Due Diligence

A fragmented CDD program can significantly increase the level of money laundering and terrorist financing risk a financial organization faces. One way to ensure that financial organizations implement a strong CDD program is to consolidate and streamline account opening and ongoing monitoring processes across the organization, both domestically and globally, when applicable.

Intergovernmental bodies have recognized the importance of implementing a consolidated CDD process and provided specific guidance to financial organizations. According to the Basel Committee, a global risk-management program for CDD should incorporate consistent identification and monitoring of customer accounts globally across business lines and geographical locations, as well as oversight at the parent level, in order to capture instances and patterns of unusual transactions that might otherwise go undetected. Such comprehensive treatment of customer information can significantly contribute to a organization's overall reputational, concentration, operational, and legal risk management through the detection of potentially harmful activities.

Financial organizations should aim to apply their customer acceptance policy, procedures for customer identification, process for monitoring high-risk accounts, and risk-management framework on a global basis to all of their offices, branches, and subsidiaries. The organization should clearly communicate these policies and procedures through ongoing training and regular communications, and it should conduct monitoring and testing to ensure compliance with the policies and procedures.

Each office, branch, and subsidiary should be capable of complying with the minimum identification and accessibility standards applied by the parent. However, some differences in information collection and retention may be necessary across jurisdictions to conform to local regulatory requirements and relative risk factors, such as areas that pose higher levels of risk related to money laundering, terrorist financing, and corruption.

When the minimum CDD standards of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two. When this is not practical, the organization should confer with its home office and attorneys to implement appropriate and effective CDD standards.

Monitoring and Screening

Economic Sanctions

Economic sanctions are a way to influence the behavior of a jurisdiction or group by financially isolating it as the "target." Increasingly, countries are using economic sanctions instead of military force as an instrument of foreign policy.

Sanctions can generally fall into one of the following categories:

- **Targeted sanctions:** Aimed at specific, named individuals, such as key leaders in a country or territory; named terrorists; significant narcotics traffickers; and proliferators of WMD. These sanctions often include the freezing of assets and travel bans, when possible.
- **Sectoral sanctions:** Aimed at key sectors of an economy to prohibit a very specific subset of financial dealings within those sectors to impede future growth
- **Comprehensive sanctions:** Generally prohibit all direct and indirect import/export, trade brokering, financing, and facilitating of most goods, technology, and services. Comprehensive sanctions are often aimed at regimes that are responsible for gross human rights violations and nuclear proliferation.

Governments impose economic sanctions on state and non-state actors for the purpose of altering the behavior that threatens the interests of the government or violates international norms of behavior.

Most jurisdictions impose sanctions regimes, particularly to comply with sanctions imposed by the United Nations and, for members, the European Union. With similar goals in their application, there is expected overlap in the sanctions applied by these bodies.

United Nations

UN sanctions are managed by the UN Security Council committees. The UN Security Council can take actions to maintain and restore international peace and security under Chapter VII of the *United Nations Charter*. Sanctions measures, under Article 41, encompass a broad range of enforcement options that do not involve the use of armed force. Security Council sanctions take several different forms in pursuit of a variety of goals. The measures range from comprehensive economic and trade sanctions to more targeted measures, such as arms embargoes, travel bans, and financial or commodity restrictions. The Security Council applies sanctions to support peaceful transitions, deter nonconstitutional changes, constrain and deter terrorism, protect human rights, and promote nonproliferation.

European Union

Article 215 of the Treaty on the Functioning of the European Union provides a legal basis for the interruption or reduction, in part or completely, of the EU's economic and financial relations with one or more third countries (i.e., countries outside the EU), when such restrictive measures are necessary to achieve the objectives of the Common Foreign and Security Policy. In general terms, the EU imposes its restrictive measures to bring about a change in policy or activity by the target country, part of a country, government, entities, or individuals. The measures are preventive, nonpunitive instruments that allow the EU to respond swiftly to political challenges and developments. The EU wields measures in support of human rights and democracy objectives in the absence of a United Nations mandate and has supplemented UN sanctions to stop nuclear proliferation in Iran and North Korea.

United States

One of the most widely known sanctions lists is OFAC's Specially Designated Nationals and Blocked Persons (SDN) list. Updated often, the SDN list includes thousands of names of individuals and businesses, as well as aircraft and ships (vessels) from more than 150 countries, which the US government considers to be terrorists, international narcotics traffickers, and other criminals covered by US foreign policy and trade sanctions. Similar to the UN and EU, OFAC

applies sanctions to deter nonconstitutional changes, constrain and deter terrorism, and protect human rights.

Under sanctions programs administered by OFAC, all US citizens and companies, including foreign subsidiaries and affiliates owned or controlled by US companies, are prohibited from providing property, or an interest in property, to a sanctions target when a general or specific license has not been issued. This includes individuals, companies, property, countries (e.g., North Korea, Syria, Cuba, and Iran) that are subject to a sanctions program. Depending on the specific program, action might involve blocking (or freezing) a transaction or rejecting or returning a transaction.

OFAC is not a supervisory agency, but it works closely with supervisory agencies at both the federal and state levels. During examinations of financial organizations, supervisory examiners review OFAC compliance efforts, including policies and procedures, training, testing, and tuning of screening systems, to determine a financial organization's ability to effectively detect SDNs and entities that are sanctioned within all of OFAC's programs—even entities that are not specially designated—and to comply with OFAC's sanctions programs. If a financial organization is found to have weak OFAC controls, is engaged in activity with an entity identified on the SDN list, or is sanctioned under any OFAC sanctions program, federal and state examiners and OFAC may take actions, including, but not limited to, issuing monetary penalties, criminal penalties, and regulatory actions (e.g., Written Agreements and Matters Requiring Attention).

The sanctions programs are governed by several laws and regulations and are subject to change; therefore, sanctions compliance requires a specialized skill set and constant attention to the changing nature of sanctions.

Sanctions List Screening

Before a financial organization starts doing business with a new customer or engages in certain transactions (e.g., international wire payments), it should review the various country sanctions program requirements, as well as published lists of known or suspected terrorists, narcotics traffickers, and other criminals, for potential matches.

Organizations subject to sanctions compliance are required to screen customers and transaction records against periodically updated lists that

include individuals and entities designated or identified by governmental bodies. Sanctions lists identify terrorists, terrorist organizations, and supporters of terrorism, as well as individuals and entities subject to targeted, sectoral, and comprehensive sanctions.

Financial organizations must be alert to transactions that involve parties identified on a sanctions list. This can be difficult, particularly because it involves screening customer lists for people whose names are not originally in Roman characters, such as suspected terrorists from Middle Eastern countries and sanctions lists in Asian countries. For example, most of the names of designated terrorists on the OFAC SDN list also include numerous “also known as” alternatives. Although some names might be aliases, others are confusing because the naming conventions are not understood. An understanding of Arab naming conventions and protocols can help alleviate the confusion.

Below are some helpful tips:

- When Arabic names are written in another alphabet, the spelling might vary. For example, “Mohammed” might be written as “Mohamed” or “Mohamad.”
- Arabic names are typically long. A person’s second name is the father’s name. A "bin" or "ibn" preceding the name indicates “son of.” If a family name is included at the end, it will sometimes be preceded by "al."
- There is widespread use of certain names, such as Mohamed, Ahmed, Ali, and names with the prefix Abd- or Abdul, which means servant of, and is followed by one of 99 suffixes used to describe God.
- Many Arabic names begin with the word "Abu." If it is a first name, it is probably not the person’s given name, because "Abu" means "father of." Abu followed by a noun means “freedom” or “struggle,” and it is used by both terrorists and legitimate political leaders. Only when Abu is a prefix of a surname should it be accepted as a given name.

Politically Exposed Persons Screening

Although financial organizations take measures to develop robust procedures and screening processes to comply with sanctions and other customer screening requirements, these controls sometimes fail to detect suspicious high-risk individuals and businesses that organizations should avoid. For example, intergovernmental bodies, such as FATF in its 40 Recommendations, explicitly reference PEPs, and government regulations, specifically the EU's Fourth Directive, explicitly detail requirements related to PEPs. However, there is no simple way to identify PEPs and their associates.

The problem is the lack of available and useful information about the identity of PEPs around the world. There are many private providers that offer PEP databases; however, the information contained in them and the ability to positively match customers with PEPs on a database can be challenging. In addition, as increased scrutiny continues to be placed on PEPs, they have become more creative in finding ways to avoid detection, such as opening accounts in the names of corporations (e.g., shell companies) in offshore jurisdictions instead of in their own names or the names of close family members. On the other hand, considering geographical issues, the size and nature of an account, and the purpose of an account might raise PEP-related issues.

There are some publicly available sources of information that can be used to help identify PEPs and their associates. Transparency International, a global, nongovernmental organization devoted to combating corruption, publishes the Corruption Perceptions Index, which is useful in focusing on high-risk jurisdictions. Some government agencies, such as the US Central Intelligence Agency, publish lists of heads of state and cabinet members of foreign governments. However, these lists do not provide all relevant information related to PEPs that would assist in identifying them. For example, they do not include unique identifiers, such as date of birth or address, which poses significant operational constraints, particularly at large retail financial organizations.

Accepting corruption proceeds from PEPs constitutes money laundering in the United States. Under some countries' laws, it may be a violation of its sanctions rules. Because it is difficult to identify these parties, it is important to have strong CDD and monitoring controls. It is also important to continually review and update customer screening and sanctions programs. This includes updating procedures, tuning, and testing screening tools and training staff.

Know Your Employee

Financial organizations and businesses have learned at great expense that an insider can pose the same money laundering threat as a customer. It has become clear in the AML/CFT field that equivalent programs to know your customer and know your employee (including contractors and third-party vendors who support AML controls) are essential.

A Know Your Employee (KYE) program ensures that an organization has the means to understand an employee's background, conflicts of interest, and susceptibility to money laundering complicity. Policies, procedures, internal controls, job descriptions, levels of authority, compliance with personnel laws and regulations, accountability, monitoring, dual control, and other deterrents should be firmly in place. Additionally, codes of conduct and ethics should specify mandatory requirements to report suspicious activity to the MLRO and that failure to comply subjects an employee to disciplinary action and possible employment termination.

Background screening of prospective and current employees and vendors, especially for criminal history and ties to negative media, is essential to prevent unwanted relationships and identify employees that should be terminated. The US Federal Deposit Insurance Corporation (FDIC) provides guidance on employee screening in its paper, *Pre-Employment Background Screening: Guidance on Developing an Effective Pre-Employment Background Screening Process*.

Background screening can be an effective risk-management tool that provides management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. Used effectively, pre-employment background checks can reduce turnover by verifying that the potential employee has the requisite skills, certification, license, or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. An organization should also verify that contractors and vendors are subject to screening procedures similar to its own and include anti-corruption compliance clauses in agreements.

Developing and implementing an effective screening process can be costly. However, without such a process, an organization might incur significant expenses in recruiting, hiring, training, and ultimately terminating unqualified individuals.

Sometimes, regulations prohibit a person who has been convicted of a crime involving dishonesty or money laundering from becoming or continuing as an institution-affiliated party; owning or controlling, directly or indirectly, an institution; or otherwise participating, directly or indirectly, in the conduct of the affairs of an institution without the prior written consent of the regulator. Consultants who take part in the affairs of a financial organization could be subject to this requirement, too.

Therefore, pre-employment background screening should be established by all financial organizations, which, at a minimum, reveals information regarding a job applicant's criminal convictions. Sometimes, the level of screening should be increased. The sensitivity of the position and the access level of an individual employee might warrant additional background screening, which should include verification of references, experience, education and professional qualifications, according to the FDIC. The Monetary Authority of Singapore's guidelines on employee hiring also include screening against ML/TF information sources, bankruptcy searches, and credit history checks.

Just as management verifies the identity of customers, it should also verify the identity of job applicants. Once the person is hired, an ongoing approach to screening should be considered for specific positions, as circumstances change or as needed for a comprehensive review of departmental staff over a period of time. Management should also establish policies that address what to do when screening uncovers information contrary to what the applicant or employee provided.

An organization can perform fingerprint checks periodically for employees in sensitive positions, and contract with a vendor to conduct extensive background checks when employees are being considered for promotion to high-level positions. Without such screening procedures in place, financial organizations risk violating the prohibition against employing statutorily disqualified individuals. The extent of the screening depends on the circumstances, with reasonableness being the standard.

In the UK, the Centre for the Protection of National Infrastructure (CPNI) publishes informative guidelines regarding insider threat and risk management. It includes examples of how insider threats and data leakages can have devastating effects on an organization. Within financial organizations, this could include abuse of pre-market information only known by insiders. Many banks these days train their staff how to treat data in a transparent, customer-centric, and law-abiding manner.

Regularly repeated training of employees regarding what is expected from them should be part of typical on-the-job training. With social media being an important day-to-day communication form for both private people and organizations, KYE programs might also require organizations to monitor what employees and other insiders mention and like on their social media accounts. Social media accounts and posts on these accounts can provide ample information regarding how a person might behave in an organization.

KYE (Case example: Citigroup Global Markets Inc.)

The Financial Industry Regulatory Authority (FINRA) regulates brokerage firms doing business with the public in the US. In July 2019, it fined Citigroup Global Markets Inc. (CGMI) US$1.25 million. FINRA found that CGMI failed to conduct timely and adequate background checks on more than 10,000 employees and may not have fingerprinted all required employees over a seven-year period.

US federal securities laws require broker-dealers to perform background screening and to fingerprint certain employees. These “know your employee” requirements help determine if a person has a statutory disqualification that would prevent them from being associated with a FINRA member firm without explicit regulatory approval.

The failure to implement these supervisory controls and procedures prior to employment meant that CGMI did not determine whether the individuals it hired were subject to statutory disqualification. In fact, FINRA found that CGMI employed or associated with three individuals who were subject to statutory disqualification due to previous criminal convictions.

Background checks, or background screening, are an important part of an organization’s know -your employee (KYE program). The purpose of a KYE program is to ensure an institution does not compromise the financial system by employing or associating with individuals with disqualifying criminal or regulatory histories. Depending on the employer's risk appetite, screening is typically completed before employment, with other regulatory requirements completed before onboarding.

Regulators expect organizations to serve as responsible gatekeepers that protect the financial system, themselves, their customers, and their investors from criminals.

This case highlights the importance of regulatory expectations and requirements for institutions concerning employment practices. Your organizations need to know the requirements in your jurisdictions. Your organization needs to develop and implement risk-based KYE frameworks to ensure potential employees are properly screened and fingerprinted. These practices protect the institution, customers, investors, and the financial system.

Key takeaways

- Know your regulatory requirements for KYE.
- Effective KYE require background checks and fingerprinting.
- Use a risk-based approach to the timing of background checks and other pre-employment requirements.
- KYE protects regulated companies, their customers and investors, and the financial system.

Suspicious and Unusual Transaction Monitoring and Reporting

Proper due diligence could require compliance personnel to gather further information regarding a customer or transaction before deeming it suspicious and filing an SAR. Although there are no hard and fast rules regarding what constitutes suspicious activity, employees of financial organizations should watch for activity that might be inconsistent with a customer's source of income or regular business activities.

Because financial organizations process thousands of transactions each day, their systems for monitoring and reporting suspicious activity should be risk-based and determined by factors such as the organization's size, the nature of its business, its location, the frequency and size of transactions, and the types and geographical locations of its customers.

Generally, the core operating system of a financial organization maintains significant customer data and can be utilized to generate specific internal reports that are useful for discovering possible money laundering and terrorist financing.

Examples of these reports include:

- Daily cash activity exceeding the country's reporting threshold
- Daily cash activity just below the country's reporting threshold (to identify possible structuring)
- Cash activity aggregated over a period of time (e.g., individual transactions over a certain amount or totaling more than a certain amount over a 30-day period, to identify possible structuring);
- Wire transfer reports/logs with filters using amounts and geographical factors
- Monetary instrument logs/reports
- Check kiting/drawing on uncollected funds with significant debit/credit flows
- Significant change reports
- New account activity reports

Although reporting procedures vary from country to country, a typical suspicious or unusual transaction reporting process within a financial organization as part of its AML/CFT program includes:

- Procedures to identify suspicious and unusual transactions and activity through various channels, including employee observations and identification, inquiries from law enforcement, and alerts generated by transaction monitoring systems
- Formal evaluation of each instance and continuation of unusual transactions and activity
- Documentation of the SAR reporting decision (i.e., whether or not a report was filed with authorities)
- Procedures to periodically notify senior management or the board of directors of SAR filings
- Employee training on detecting suspicious transactions and activity

Most countries that require SAR reporting prohibit disclosing the filing to the subject of the report (i.e., tipping off). In the United States, a financial organization and its directors, officers, employees, and agents may not notify any person involved in the transaction that it has been reported. Most laws also grant immunity from civil liability (i.e., safe harbor) to the filing organization and its employees.

The US has even made it illegal to reveal information that would lead to knowledge of the existence of a SAR. This includes not only a prohibition on divulging the SAR itself, but also the fact that a SAR was or was not filed. For example, if an employee of a financial organization were asked whether it had filed a SAR, a failure to answer could indirectly indicate that a SAR had been filed. The confidentiality of SARs is a critical aspect of the whole reporting program, because it protects financial organizations from being intimidated from filing reports. After all, the reports are meant to provide useful information to law enforcement, and the threat of lawsuits by criminals should not deter financial organizations from fulfilling this important duty.

Strong recordkeeping procedures are key to managing any regulatory and legal implications of SAR filing. National laws and regulations usually dictate the length of time financial organizations and businesses must maintain records, the types of records that must be stored, and how they should be provided to regulatory and law enforcement personnel upon request.

There is no international clearinghouse for keeping SARs, but FIUs in various countries often publish reports on how many SARs are filed each year, which areas are filing the most reports, and what the suspicious activity and typology trends are, as well as case studies. This information provides added guidance to financial organizations operating within their jurisdiction regarding their AML/CFT obligations.

Automated AML/CFT Solutions

The sheer number of people and the volume of regulations and data involved in complying with regulations make manual AML/CFT compliance difficult, if not impossible. Most organizations have designated technology systems to automate their compliance activities, and some still undertake their efforts manually.

Appropriately functioning technology can equip financial organizations with improved defenses in the fight against financial crime by providing the following:

- **Automated customer verification:** Using third-party databases to compare information provided by a customer with source data
- **Watch list filtering:** Screening new accounts, existing customers, beneficiaries, and transaction counterparties against terrorist, criminal, and other blocked-persons sanctions and/or watch lists
- **Transaction monitoring:** Scanning and analyzing transactional data for potential money laundering activity
- **Automation of regulatory reporting:** Filing SARs, CTRs, and other regulatory reports with the government
- **Case management:** Providing a dashboard feature to view customer KYC, transaction history, investigations undertaken, and regulatory filings filed on a customer
- **Audit trail:** Documenting steps taken to demonstrate compliance efforts to auditors and supervisory authorities

Automation is used for more than increased efficiency and control. It also can reflect a company's commitment to meet or exceed compliance requirements. A byproduct of this commitment is that regulators can receive prompt, concise, and properly formatted information.

Many software companies offer technology dedicated to combat laundering, and some organizations have internally generated electronic systems. Before designing an AML/CFT compliance program or purchasing new technology, financial organizations should review the feasibility, costs, and benefits to be derived from each course of action.

Some financial organizations choose to hire a vendor to provide AML/CFT software packages. Many organizations use a Request for Proposal (RFP) method in which they issue RFPs to software providers that might be qualified to participate. An RFP lists project specifications and application procedures. The objective of the RFP is to select a system that will assist the organization in completing its responsibilities under applicable money laundering regulations. The system(s) can help identify potentially high-risk customers, accounts, and transactions; aid in conducting, managing, and documenting any resulting investigations; and streamline the completion and filing of required SARs.

Most organizations seek a partner with a longstanding commitment to stay ahead of the rapidly changing regulatory landscape and experience that reflects flexibility, agility, and urgency in delivering features that improve its clients' efficiency in monitoring the right transactions and investigating the right clients. Ideally, the system is flexible, fast, and efficient to deploy. It should allow the organization to navigate seamlessly around client relationships, accounts, and transactions across a variety of product lines and systems, including deposits, wires, transfers, loans, trust, brokerage, letters of credit, and check-imaging applications. A single view into customer relationships is of paramount importance in delivering efficient, reliable, and instant access to information. Each organization needs to identify the vendor that best meets its needs. During the RFP process, most organizations form evaluation teams comprising management staff from the compliance, operations, technology, and business departments. The team, facilitated by the project manager, is responsible for reviewing and scoring all responses to the RFP.

Determining the most applicable system for a financial organization depends on its customer base, size, and products and services offered. In general, it should consider the following capabilities of the system during its assessment process:

- Ability to monitor transactions and identify anomalies that might indicate suspicious activity
- Ability to gather CDD information for new and existing customers, score customer responses, and store CDD data for subsequent use
- Ability to conduct advanced evaluation and analysis of suspicious and unusual transactions identified by the monitoring system in the context of each customer's risk profile and that of his peer group

- Ability to view individual alerts within the broader context of the customer's total activity at the organization
- Workflow features, including the ability to create a case from an alert or series of alerts, collaborate (simultaneously or serially) among multiple interested parties to view and update information, and share AML/CFT-related information across monitoring and investigating units and throughout the organization, as needed
- Ability to use data from the organization's core customer and transaction systems and databases to inform and update monitoring and case-management activities
- Ability to store and recall at least 12 months of data for trend analysis
- Ability to manage the assignment, routing, approval, and ongoing monitoring of suspicious activity investigations
- Automated preparation and filing of SARs to FIUs
- Standard and ad-hoc reporting on the nature and volume of suspicious activity investigations and investigator productivity for management and other audiences
- Enhanced ability to plan, assign, and monitor the caseload per employee of AML-related investigations
- Ability to provide comprehensive and accurate reporting of all aspects of AML compliance, including reporting to management, reporting to regulators, productivity reporting, and ad-hoc reporting
- User-friendly updating of risk-parameter settings without the need for special technical computing skills
- Tiered user-rights access for users, managers, and auditors

In addition to the above features, financial organizations should evaluate the following aspects of automated systems:

- Ease of use of the application, as well as the configuration of new and changed transaction monitoring rules
- Ease of data integration, system implementation, and configuration
- Scalability of application, i.e., the ability of the system to grow with the organization

- Extent to which the system can be supported with internal resources
- User satisfaction with hardware and software support
- Price, including initial cost and ongoing costs to sustain the system or expand its capabilities, both in terms of what the vendor will charge and how much the organization will need to spend in terms of dollars, personnel, and technology capacity

In addition to providing possible regulatory compliance solutions, automated tools can help an organization analyze how customers and other users are using its products and services. For marketing purposes, patterns of activity among types of customers and different business lines can be represented by graphs and statistical reports. Depending on an organization's needs, a variety of software products can automate these tasks—from standard analytical systems to sophisticated artificial intelligence.

Automated tools can also help with documentation management, which can be a significant burden for many financial organizations. Historically, imaging systems offered quick and paperless access to records. However, convenience is not enough. New systems can track and report the status of all documents, including those that are missing and expired. One-stop access systems can provide images, standardization, and control for documents that must be accounted for and produced for compliance purposes.

Money Laundering and Terrorist Financing Red Flags

Although there is no exhaustive list of tried-and-true suspicious activity indicators for businesses, there are many common indicators of financial crime, money laundering, and terrorist-financing activity that organizations can watch for.

Methods of money laundering have become more sophisticated as the complexity of financial relationships has grown and the paths through which funds move worldwide through financial organizations have multiplied. Worldwide terrorist threats are also a concern. Financial organizations and NBFIs play a critical part in efforts to disrupt the movement of funds used to support and carry out terrorist attacks. Although it may be difficult to detect terrorist financing transactions, there is guidance available from a variety of authoritative sources. Red flag indicator guidance should be used when building out and refining transaction monitoring programs.

The following situations might warrant additional scrutiny, as they can indicate money laundering or terrorist financing. These lists are not exhaustive, but they will help to determine whether an activity is suspicious or does not appear to have a reasonable business or legal purpose.

Unusual Customer Behavior

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses a financial organization's recordkeeping or reporting requirements with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required recordkeeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be reported.

- Customer suggests paying a gratuity to an employee.
- Customer appears to have a hidden agenda or behaves abnormally, such as declining a higher interest rate on a large account balance.
- Customer, who is a public official, opens an account in the name of a family member, who begins making large deposits that are not consistent with the known sources of legitimate family income.
- Customer, who is a student, uncharacteristically transfers or exchanges large sums of money.
- Account shows high velocity in the movement of funds, but it maintains low beginning and ending daily balances.
- Transaction involves offshore organizations whose names resemble those of well-known legitimate financial organizations.
- Transaction involves unfamiliar countries or islands that are difficult to locate on an atlas or map.
- Agent, attorney, or financial advisor acts for another person without proper documentation, such as a power of attorney.

Unusual Customer Identification Circumstances

- Customer provides unusual or suspicious identification documents or declines to produce original documents for verification.
- Customer is unwilling to provide personal background information when opening an account.
- Customer tries to open an account without identification, references, or complete local address.
- Customer's permanent address is outside of the organization's service area.
- Customer's home or business telephone is disconnected.
- Customer does not want a statement of his account or any other mail to be sent to him.

- Customer asks many questions about how the financial organization shares information about the identification of its customers.
- A business customer is reluctant to provide complete information about the nature and purpose of its business, anticipated account activity, and other details about the business, or to provide financial statements or other documents about a related business entity.
- Customer provides no record of past or present employment on a loan application.
- Customer's Internet Protocol (IP) address or online device tracing does not match the identifying information or government-issued identification provided during online registration.

Unusual Cash Transactions

- Customer makes a large cash deposit without having counted the cash.
- Customer frequently exchanges small bills for large bills.
- Customer's cash deposits often contain counterfeit bills or musty or extremely dirty bills.
- Customer enters the bank with another customer, and they go to different tellers to conduct currency transactions under the reporting threshold.
- Customer makes a large cash deposit containing many high-denomination bills.
- Customer opens several accounts in one or more names, and then makes several cash deposits under the reporting threshold.
- Customer withdraws cash in amounts under the reporting threshold.
- Customer withdraws cash from one of her accounts and deposits it into another account the customer owns.
- Customer conducts unusual cash transactions through night deposit boxes, especially large sums that are not consistent with the customer's business.

- Customer makes frequent deposits or withdrawals of large amounts of currency for no apparent business reason or for a business that generally does not generate large amounts of cash.
- Customer conducts large cash transactions at different branches on the same day or coordinates other individuals to do so on his behalf.
- Customer deposits cash into several accounts in amounts below the reporting threshold, consolidates the funds into one account, and then wire transfers them abroad.
- Customer attempts to take back a portion of a cash deposit that exceeds the reporting threshold after learning that a CTR will be filed.
- Customer conducts several cash deposits below the reporting threshold at ATMs.
- Corporate account has deposits or withdrawals primarily in cash, rather than checks.
- Customer frequently deposits large sums of cash wrapped in currency straps.
- Customer frequently purchases monetary instruments with cash in amounts lower than the reporting threshold.
- Customer conducts an unusual number of foreign currency exchange transactions.
- Customer conducts foreign currency exchange transactions/currency swaps without seeming to care about the margins.
- A noncustomer deposits cash into a customer account, which is subsequently withdrawn at a different geographic location.

Unusual Noncash Deposits

- Customer deposits a large number of traveler's checks, often in the same denominations and in sequence.
- Customer deposits large numbers of consecutively numbered money orders.

- Customer deposits checks and/or money orders that are not consistent with the stated purpose of the account or nature of business.
- Customer deposits a large number of third-party checks.
- Deposited funds are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

Unusual Wire Transfer Transactions

- Wire transfers are sent or received from the same person to or from different accounts.
- Customer uses message type (MT) 202 for a covered payment in SWIFT messaging to obscure wire transfer information.
- Nonaccount holder sends wire transfer with funds that include numerous monetary instruments, each in an amount under the reporting threshold.
- An incoming wire transfer includes instructions to convert the funds to cashier's checks and mail them to a nonaccount holder.
- Wire transfer activity occurs to and from secrecy havens or high-risk geographic locations without apparent business reason or inconsistent with a customer's transaction history.
- An incoming wire transfer is followed by the immediate purchase by the beneficiary of monetary instruments for payment to another party.
- There is an increase in international wire transfer activity in an account with no history of such activity or when the stated business of the customer does not warrant it.
- Customer frequently shifts purported international profits by wire transfer out of the country.
- Customer receives many small incoming wire transfers and then orders a large outgoing wire transfer to another country.
- Customer deposits bearer instruments followed by instructions to wire the funds to a third party.
- An account in the name of a currency exchange house receives wire transfers and/or cash deposits under the reporting threshold.

Unusual Safe Deposit Box Activity

- Customer spends an unusual amount of time in the safe deposit box area, possibly indicating the safekeeping of large amounts of cash.
- Customer often visits the safe deposit box area immediately before making cash deposits of sums under the reporting threshold.
- Customer rents multiple safe deposit boxes.

Unusual Activity in Credit Transactions

- A customer's financial statement makes representations that do not conform to accounting principles.
- A transaction is made to appear more complicated than necessary by the use of nonsensical technical terms, such as emission rate, prime bank notes, standby commitment, arbitrage, and hedge contracts.
- Customer requests loans either made to offshore companies or secured by obligations of offshore banks.
- Customer suddenly pays off a large problem loan with no plausible explanation regarding the source of funds.
- Customer purchases certificates of deposit and uses them as collateral for a loan.
- Customer collateralizes a loan with cash deposits.
- Customer uses cash collateral located offshore to obtain a loan.
- Customer's loan proceeds are unexpectedly transferred offshore.

Unusual Commercial Account Activity

- Business customer presents financial statements that are noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.

- Retail business that provides check-cashing services does not make withdrawals of cash against check deposits, possibly indicating that it has another source of cash.
- Small business makes deposits that are inconsistent with its expected activity or receives funds from other unrelated businesses.
- Customer maintains an inordinately large number of accounts for the type of business purportedly being conducted.
- Corporate account shows little or no regular, periodic activity.
- A transaction includes circumstances that would cause a banker to reject a loan application because of doubts about the collateral.
- Multiple high-value payments or transfers occur between shell companies with no apparent legitimate business purpose.
- Transacting businesses share the same address, provide only a registered agent's address, or raise other address-related inconsistencies.

Unusual Trade Financing Transactions

- Customer seeks trade financing on the export or import of commodities with stated prices that are substantially higher or lower than those in a similar market situation or environment.
- Customer requests payment of proceeds to an unrelated third party.
- Customer presents significantly amended letters of credit without reasonable justification or changes the location of payment or the beneficiary just before payment is made.
- Customer changes the place of payment in a letter of credit to an account in a country other than the beneficiary's stated location.
- Customer's standby letter of credit is used as a bid or performance bond without the typical reference to an underlying project or contract or designates unusual beneficiaries.
- Letter of credit is inconsistent with customer's business.
- Letter of credit covers goods that are in little demand in importer's country.

- Letter of credit covers goods that are rarely, if ever, produced in the exporter's country.
- Documents arrive without title documents.
- Letter of credit is received from a country that is considered high risk for money laundering.
- Obvious overpricing or underpricing of goods and services.
- The structure of a transaction appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Commodities are shipped through one or more jurisdictions for no apparent economic or logistical reason.
- Transaction involves the use of repeatedly amended or frequently extended letters of credit.
- Size of a shipment appears inconsistent with the regular volume of business of the importer or exporter.

Unusual Investment Activity

- Customer uses an investment account as a pass-through vehicle to wire funds to offshore locations.
- Investor seems disinterested in the typical decisions made about investment accounts, such as risk, commissions, fees, and the suitability of the investment vehicles.
- Customer wants to liquidate a large position through a series of small transactions.
- Customer deposits cash, money orders, traveler's checks, or cashier's checks in amounts under the reporting threshold to fund an investment account.
- Customer cashes out annuities during the free-look period or surrenders the annuities early.

Other Unusual Customer Activity

- Customer conducts an unusually high number of transactions over the internet or by telephone.
- Customer purchases several open-end prepaid cards for large amounts, inconsistent with normal business activity.
- Funds withdrawn from accounts are not consistent with the normal business or personal activity of the account holder or include transfers to suspicious international jurisdictions.
- Customer uses a personal account for business purposes.
- Customer repeatedly uses bank or branch locations geographically distant from the customer's home or office without sufficient business purpose.

Unusual Employee Activity

- Employee exaggerates the credentials, background, financial ability, or resources of a customer in written reports the bank requires.
- Employee is involved in an excessive number of unresolved exceptions.
- Employee lives a lavish lifestyle that could not be supported by her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy (e.g., removes the name of a high-risk person from a wire, known as wire stripping).
- Employee uses company resources to further private interests.
- Employee facilitates transactions in which the identity of the ultimate beneficiary or counterparty is undisclosed.
- Employee avoids taking periodic vacations.
- Employee functions performed by vendors or contractors have unusual billing or payment terms.

To mitigate these risks, employees should be made aware that willfully violating AML requirements can be a criminal offense, for which the individual could be subject to fines and/or imprisonment.

Unusual Activity in a Money Remitter or Currency Exchange House Setting

- Customer uses money orders, traveler's checks, or funds transfers in an unusual manner.
- Two or more people work together in transactions.
- Transaction is altered to avoid filing a CTR.
- Customer comes into the bank frequently to purchase less than US$3,000 in instruments each time (or whatever the local recordkeeping threshold is).
- Transaction is altered to avoid completing a record of funds transfer, money order, or traveler's checks of US$3,000 or more (or whatever the local recordkeeping threshold is).
- The same person uses multiple locations in a short time period.
- Two or more people use the same identification.
- One person uses multiple identification documents.

Unusual Activity for Virtual Currency

- Repeated receipt of funds transfers from virtual currency exchanges is inconsistent with customer profile.
- Multiple transfers are made to one common end user.
- Transactions involving virtual currency exchanges are followed within a brief time by funds transfers to high-risk geographies or ATM withdrawals in high-risk geographies.
- Purchase of virtual currency quickly follows the receipt of funds transfers from unconnected third parties.
- Multiple accounts are used to collect and funnel funds to a small number of virtual currency accounts.

- Multiple purchases of virtual currency are at or just below US$3,000, or the local recordkeeping requirement.
- Key words entered into the transaction could relate to the sale of suspicious products.

Unusual Activity in an Insurance Company Setting

- Cash payments are made on insurance policies.
- Customer overfunds an insurance policy and then moves money out of it, despite early-withdrawal fees.
- Customer uses multiple currency equivalents (e.g., cashier's checks and money orders) from different sources to make insurance policy or annuity payments.
- Customer purchases products that appear outside his normal range of financial wealth or estate planning needs.
- Customer makes an early withdrawal of insurance bond, disregarding applicable fees.
- Customer requests refunds during a policy's legal cancellation period or free-look period.
- Policy premiums are paid from abroad or by a third party, especially from an offshore financial center.
- A policy stipulates the periodic payment of premiums in large amounts.
- Customer changes the named beneficiary of a policy to a person with no clear relationship to the policyholder.
- There is a lack of concern for significant tax or other penalties assessed when cancelling a policy.
- Insurance bonds that were originally subscribed to by an individual in one country are redeemed by a business entity in another country.

Unusual Activity in a Broker-Dealer Setting

In 2002, the predecessor to FINRA, the US National Association of Securities Dealers (NASD), a self-regulatory organization that oversaw the NASDAQ Stock Market under the authority of the US Securities and Exchange Commission, offered in its Special NASD Notice to Members signs of suspicious activity to the securities field, including:

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information, or is otherwise evasive regarding that person or entity.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment that is followed shortly thereafter by a request to liquidate the position and transfer the proceeds from the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in a manner that avoids the organization's typical documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S (Reg S) stocks, and bearer bonds, which, although legitimate, have been used in connection with fraudulent schemes and money laundering activity.
- The customer's account shows an unexplained high level of activity with very low levels of securities transactions.

Unusual Real Estate Activity

- Borrower/buyer submits invalid documents in order to cancel mortgage obligations or pay off her loan balances(s).
- The same notary public and/or other authorized representative works with and/or receives payments from an unusually high number of borrowers.
- Certified checks, cashier's checks, or noncash item checks are falsified and drawn against a borrower/buyer's account, rather than from the account of a financial organization.
- Borrower/buyer applies for a loan for a primary residence, he but does not reside in the new primary residence, as indicated on the loan application. Other individuals occupy the borrower/buyer's new primary residence, indicating the property is being used as a secondary residence or income-generating property.
- Borrower/buyer requests refinancing for her primary residence, although public and personal documents indicate that she resides somewhere other than the address on the loan application.
- Low appraisal values, non-arms-length relationships between short-sale buyers and sellers, and previous fraudulent sale attempts in short-sale transactions are unusual real estate activities.
- The agent of the buyer and/or seller in a mortgage transaction is unlicensed.
- Past misrepresentations were made by the borrower/buyer in attempts to secure funding, property, refinance, and/or short sales.
- Improper/incomplete file documentation, including borrower/buyer reluctance to provide more information and/or unfulfilled promises to provide more information, represents unusual activity.
- The apparent resubmission of a rejected loan application with key borrower/buyer details modified from the individual borrower to company/corporation could represent the same person attempting to secure a loan fraudulently through a straw-borrower or nonexistent person.

- Borrower/buyer attempts to structure currency deposits and withdrawals, or otherwise hides or disguises the true value of assets, in order to qualify for loan-modification programs intended for homeowners in financial distress.
- There is a request from third-party affiliates on behalf of distressed homeowners to pay fees in advance of the homeowner receiving mortgage counseling, foreclosure avoidance, loan modification, or other related service.
- A third party solicits distressed homeowners for purported mortgage counseling, foreclosure avoidance, loan modification, or other related services. These third parties might also claim to be associated with legitimate mortgage lenders, the US government, or a US government program.

Unusual Activity for Dealers of Precious Metals and Other High-Value Items

The FATF Report, *Money Laundering and Terrorist Financing Through Trade in Diamonds*, describes transactional and other red flag indicators related to trade practices, including:

- Diamonds originate from a country where there is limited production or no diamond mines at all.
- Trade is conducted in large volumes with countries that are not part of the diamond pipeline.
- The volume of purchases and/or imports grossly exceeds the expected sales amount.
- Gold bars, coins, and loose diamonds are sold from a jewelry store (i.e., retail).
- There is an increase in the volume of activity in a diamond dealer's account, despite a significant decrease in the industry-wide volume.
- An intermediary located abroad facilitates the selling and buying of diamonds between two local companies (lack of business justification and/or uncertainty as to actual passage of goods between companies).

- Payments related to the appearance of rare or unique diamonds are made in the international market outside of known trading procedures (e.g., Argyle's rare pink diamond appearing in the international marketplace outside of the annual tender process).
- A single bank account is used by multiple businesses.
- A single bank account has multiple deposit handlers (retail and wholesale).
- Third parties are used to deposit funds into a single dealer's or multiple diamond dealers' accounts.
- Financial activity is inconsistent with practices in the diamond trade.
- Deposits or transfers to a diamond dealer's account from foreign companies are followed by the immediate transfer of similar amounts to another jurisdiction.
- Open export is settled by offsetting to, and receiving payment from, a third party.
- Funds are received/transferred for import/export, and the ordering customer/beneficiary is an MSB.
- The name of receiver in the payment from the diamond dealer is not the exporter/supplier.

Unusual Activity Indicative of Trade-Based Money Laundering

- Payment is made by virtually any method (e.g., cash, wire, check, or bank drafts) by a third party with no connection to the underlying transaction.
- Structured currency deposits are made to individual checking accounts with multiple daily deposits to multiple accounts at different branches of the same bank on the same day.
- There are discrepancies between the description of goods or commodity in the invoice and the actual goods shipped.
- Letters of credit are amended without justification.

- There is no apparent business relationship between the parties and transactions.
- Frequent transactions are conducted in round or whole dollars.
- Funds are transferred into an account and moved to a high-risk country in the same amount.
- Companies operate in jurisdictions where their business purpose is not fully understood, and there are difficulties in determining ownership.
- There is a lack of appropriate documentation to support transactions.
- Negotiable instruments are used to fund transactions in sequential numbers and/or have missing payee information.

Unusual Activity Indicative of Human Smuggling

According to FinCEN, the following are red flags for human smuggling:

- Multiple wire transfers, generally kept below the US$3,000 reporting threshold, are sent from various locations across the United States to a common beneficiary located in a US or Mexican city along the southwest border.
- Multiple wire transfers are conducted at different branches of a financial organization to or from US or Mexican cities along the southwest border on the same day or on consecutive days.
- Money flows do not fit common remittance patterns:
    - Wire transfers that originate from countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, and Honduras) are directed to beneficiaries located in a US or Mexican city along the southwest border.
    - Beneficiaries receive wire transfers from countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, and Honduras), but they are not nationals of those countries.
- Unusual currency deposits into US financial organizations are followed by wire transfers to countries with high migrant populations (e.g., Mexico,

Guatemala, El Salvador, and Honduras) in a manner that is inconsistent with expected customer activity. This might include sudden increases in cash deposits, rapid turnover of funds, and large volumes of cash deposits with unknown sources of funds.

- Multiple apparently unrelated customers send wire transfers to the same beneficiary, who might be located in a US or Mexican city along the southwest border. These customers might also use similar transactional information, including, but not limited to, common amounts, addresses, and phone numbers. When questioned to the extent circumstances allow, the customers might have no apparent relation to the recipient of the funds or know the purpose of the wire transfers.
- A customer's account appears to function as a funnel account, whereby cash deposits (often kept below the US$10,000 reporting threshold) occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.
- Checks deposited from a possible funnel account appear to be pre-signed, bearing different handwriting in the signature and payee fields.
- A customer who is not in a cash-intensive industry frequently exchanges small denomination for larger denomination bills. This type of activity might occur when smugglers prepare proceeds for bulk cash shipments.
- When customer accounts near the southwest border are closed due to suspicious activity, new customers might begin transacting on behalf of the customers whose accounts have been closed, as a means to continue illicit activities. In this case, new accounts often reflect activity similar to that of the closed accounts; transactions might be frequently occurring, currency-intensive, and involve individuals who used to receive/send funds from/to accounts previously closed due to suspicious activity.
- Customer exhibits an unexplained/unjustified lifestyle that is not commensurate with his employment or business line, or profits/deposits are significantly greater than that of peers in similar professions/business lines.
- Inflows are largely received in cash, and substantial cash receipts are inconsistent with the customer's line of business; there is an extensive use of cash to purchase assets and conduct transactions.

Unusual Activity Indicative of Human Trafficking

According to FinCEN's *Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking—Financial Red Flags*, the following are red flags for human trafficking:

- A business customer does not exhibit normal payroll expenditures (e.g., wages, payroll taxes, and social security contributions); payroll costs might be nonexistent or extremely low for the size of the customer's alleged operations, workforce, and/or business line/model.
- Wages are substantially deducted. To the extent a financial organization is able to observe, a customer with a business might deduct large amounts from the wages of its employees, alleging extensive charges (e.g., housing and food costs), and the employees only receive a small fraction of their wages. These deductions might occur before or after the payment of wages.
- Payroll checks are cashed, but the majority of the funds are kept by the employer or deposited back into the employer's account. This activity might be detected by financial organizations that have access to paystubs and other payroll records.
- Frequent outbound wire transfers, with no business or apparent lawful purpose, are directed to countries at high risk for human trafficking or to countries that are inconsistent with the customer's expected activity.
- A customer's account appears to function as a funnel account, whereby cash deposits occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.
- Multiple apparently unrelated customers send wire transfers to the same beneficiary. These customers might also use similar transactional information, including, but not limited to, a common address and phone number. When questioned to the extent circumstances allow, the customers might have no apparent relation to the recipient of the funds or know the purpose of the wire transfers.

- Transactions are conducted by individuals and escorted by a third party (e.g., under the pretext of requiring an interpreter) to transfer funds, which seem to be their salaries, to other countries.
- Frequent payments are made to online escort services for advertising, including small posting fees to companies of online classifieds and more costly, high-end advertising and website hosting companies.
- Frequent transactions, inconsistent with expected activity and/or line of business, are carried out by a business customer in an apparent effort to provide sustenance to individuals, such as payment for housing, lodging, regular vehicle rentals, and purchases of large amounts of food.
- Payments are made to employment or student recruitment agencies that are not licensed/registered or that have labor violations.
- A customer establishes an account or visits a branch to conduct transactions while escorted by a third party (e.g., under the pretext of requiring an interpreter). The third party escorting the customer might have possession of the customer's ID.
- A common signer/custodian is used in apparently unrelated business and/or personal accounts. Similarly, common information (e.g., address, phone number, and employment information) is used to open multiple accounts in different names.
- An employer or employment agency serves as a custodian for the accounts of foreign workers or students.
- Customer exhibits an unexplained/unjustified lifestyle that is not commensurate with his employment or business line, or profits/deposits are significantly greater than that of peers in similar professions/business lines.
- Inflows are largely received in cash, and substantial cash receipts are inconsistent with the customer's line of business; there is an extensive use of cash to purchase assets and conduct transactions.

The following two red flags might signal anomalous customer activity; however, they should be applied in tandem with other indicators when determining whether transactions are linked to human trafficking:

- Transactional activity (e.g., credits and/or debits) is inconsistent with a customer's alleged employment, business, or expected activity, or transactions lack a business or apparent lawful purpose.
- Cash deposits or wire transfers are kept below US$3,000 or US$10,000 in an apparent effort to avoid recordkeeping and CTR filing requirements, respectively.

Unusual Activity Indicative of Potential Terrorist Financing

The Egmont Group reviewed 22 terrorist financing cases submitted by FIUs and identified the following financial and behavioral indicators that were most frequently associated with terrorist financing:

Behavior indicators

- Parties to the transaction (e.g., owner, beneficiary) from countries known to support terrorist activities and organizations
- Use of false corporations, including shell companies
- Inclusion of the individual on the United Nations 1267 Sanctions list
- Media reports that the account holder is linked to a known terrorist organization or engaged in terrorist activities
- Beneficial owner of the account is not properly identified
- Use of nominees, trusts, family member, or third-party accounts
- Use of false identification
- Abuse of nonprofit organizations

Indicators linked to financial transactions

- Use of funds by nonprofit organization inconsistent with the purpose for which it was established
- Transaction not economically justified, considering the account holder's business or profession
- Series of complicated transfers of funds from one person to another as a means to hide their source and intended use
- Transactions that are inconsistent with the account's typical activity
- Deposits structured below the reporting requirements to avoid detection
- Multiple cash deposits and withdrawals with suspicious references
- Frequent domestic and international ATM activity
- No business rationale or economic justifications for the transactions
- Unusual cash activity in foreign bank accounts
- Multiple cash deposits in small amounts in an account, followed by a large wire transfer to another country
- Use of multiple foreign bank accounts

Unusual Activity Indicative of Cyber Criminal Activity

Cybercrimes are crimes committed using the internet or other computer technology to target individuals. The incidence of cybercrime is growing, and it is becoming one of the most prevalent financial crimes around the world. Cybercriminals are motivated by financial or ideological goals. Some of the most common cybercrimes include:

- **Phishing Scams:** Phishing is the fraudulent practice of sending emails or texts purporting to be from a reputable company to try to obtain an individual's login credentials or personal identifiable information. This practice is done on an individual basis and in mass (bulk phishing).
- **Spear Phishing:** Similar to phishing, spear phishing messages appear to come from a trusted source that is familiar to the victim. Typically spear phishing uses information about the victim that was collected using social media.
- **Ransomware:** This is an attack conducted by a hacker in which malicious software designed to block access to a computer system is installed and not removed until a sum of money is paid.
- **Business Email Compromise (BEC):** BEC is a scam in which an attacker obtains access to a business email account and imitates an executive's identity in order to defraud the company.

FinCEN has an advisory on red flags that describes cybercrimes and the types of reviews that should be conducted when suspecting a cybercrime.

Conducting and Responding to Investigations

This chapter discusses the various channels through which financial organizations receive information with which to initiate investigations and explains the steps they should take to ensure that investigations are conducted thoroughly and effectively.

Investigations Initiated by the Financial Organization

Sources of Investigations

Investigations can be initiated from proactive monitoring for potentially suspicious activity and reactive measures taken to address regulatory findings, referrals, and other recommendations.

Common investigation initiators include:

- Regulatory recommendations and official findings
- Transaction monitoring rules designed to detect and trigger alerts on potentially suspicious activity
- Referrals from customer-facing employees regarding potentially suspicious activity
- Information obtained from internal hotlines

- Negative media information
- Receipt of a governmental subpoena, search warrant, or other law enforcement request

Regulatory recommendations and official findings

Financial organizations often initiate investigative efforts based on regulatory findings and recommendations. These efforts could result in the creation of new ongoing monitoring or serve as one-time reviews to address specific questions or observations. Most importantly, investigations that are initiated as a result of regulatory findings should be clearly documented and designed to ensure that all aspects of the findings are addressed within the time frame (if any) provided by the issuing body. Moreover, senior management or higher-level professionals should be informed of the findings of the regulatory review, the status of measures to address them, and their final disposition to ensure the financial organization appropriately remediates the findings or recommendations.

Transaction monitoring

Financial organizations should establish a program to regularly monitor transactions to proactively identify potentially suspicious activity. Common approaches to transaction monitoring include the creation of in-house, customizable transaction monitoring rules or engaging a third-party vendor to assist with the development and implementation of automated rules. Financial organizations should use a risk-based approach to designing transaction monitoring rules that considers the size of the organization, products offered, and features of those products.

The organization should also have policies and procedures for monitoring for suspicious activity and clearly specify the parameters and thresholds that are set to trigger an investigation. These policies should be regularly reviewed and updated to account for changes and enhancements to the monitoring rules program.

The Wolfsberg Group noted in its *Statement on Monitoring, Screening, and Searching* that an organization's transaction monitoring framework should be aligned to the risk of its business model, the products and services offered, and its customer base, and it should be embedded in the organization's AML

program. The document additionally discusses types of monitoring, typology reviews, and staff training.

Transaction monitoring rules should be regularly reviewed and tuned accordingly to ensure that they continue to operate as designed. Tuning practices may include evaluating the output of monitoring rules, examining specific thresholds and conducting above and below-the-line testing to determine whether rule adjustments are necessary.

Referrals from customer-facing employees

In addition to automated, ongoing transaction monitoring, financial organizations often have a mechanism by which customer-facing employees can refer matters to be investigated for potentially suspicious activity. Depending on the size of the organization, there could be manual referral processes via email or telephone, or an internal reporting system that routes the referrals to the appropriate investigative teams. For example, a financial organization might have a specific, internal, online form that can be completed by branch personnel when they identify unusual activity. Examples of such activity include a customer who structures transactions, currency that contains an odor indicative of controlled substances, and inconsistent responses by the customer to questions regarding the source of large cash deposits. Upon completion of the form by the branch, it is delivered to a designated AML/CFT compliance email address. Subsequently, the AML/CFT team reviews the activity during the normal course of its investigations process. The existence of these referral mechanisms and the types of activity that may warrant referrals should be included in employee training programs, especially for those employees on the first line of defense.

Internal hotlines

Internal hotlines are also known as ethics, compliance, and whistleblower hotlines. They allow employees to report a wide range of activity, including employee fraud, harassment, discrimination, violations of codes of conduct, theft of company property, and inappropriate gifts. The hotlines might ask the employee to provide his identity, but most allow for anonymous reporting. In either case, in most jurisdictions, the financial organization is prohibited from retaliating against the person who made a report via the hotline. The financial organization must maintain policies, procedures, and processes to

confidentially investigate the information provided through the hotline. The size and scale of a financial organization will determine the organizational recipient of the hotline information, such as legal, compliance, human resources, or corporate security.

Negative media information

Investigations can be initiated in response to notable media stories about a financial organization's customer, how a product is used in the market, a geographic location it serves, or a money laundering or terrorist event. Thus, financial organizations should develop a process to receive, review, and escalate these types of potentially high-priority triggers. It is critical to determine whether the negative information is financially risk-relevant to the organization. In some instances, financial organizations might proactively monitor media stories and initiate investigations to determine if a SAR should be filed and if further actions are necessary.

Negative news example

Receipt of a governmental subpoena or search warrant

Financial organizations often initiate investigations upon receipt of a governmental subpoena or search warrant. In either situation, the organization has two independent obligations: (1) legally fulfill the requirements of the subpoena or warrant, and (2) determine whether the activity of its customer identified in the subpoena or warrant requires the filing of a SAR.

Notably, banking regulatory agencies do not need to use subpoenas, search warrants, or other jurisdiction-specific legal mechanisms. Rather, their authority to conduct examinations includes the ability to inspect all books and records of a regulated organization.

Subpoena

Subpoenas are usually issued by grand juries that operate under the purview of a court. They empower a law enforcement agency to compel the production of documents and testimony, which allow the law enforcement agency to investigate suspicious transactions, develop evidence, and, ultimately, put together a case for prosecution.

When an organization is served with a subpoena compelling the production of certain documents or summon an individual related to its customer, the organization should ensure its senior management and/or legal counsel reviews the subpoena and independently confirms its legitimacy (e.g., to confirm that it is not an attempted fraud to obtain confidential information). If there are no grounds for contesting the subpoena, the organization should take all appropriate measures to comply with the summons or subpoena on a timely and complete basis. Failure to do so can result in adverse action and penalties for the financial organization. The financial organization should never notify the customer being investigated.

To produce documents related to governmental requests, an organization should start by appoint an employee with knowledge of the organization's files to take charge of retrieving documents for the organization. A system must be in place to ensure that all documents are located, whether they be in central files, department files, or individual files. In addition, copies of the same document in different hands should be retrieved, because some copies might have handwritten notes by the employees who received them.

If the government asks the organization to keep certain accounts open, this request should be obtained in writing under proper letterhead and authority from the government. The request should include the duration for which the account should remain open. Documentation of the request should be maintained for at least five years after the request has expired.

Search warrant

A search warrant is a grant of permission from a court for a law enforcement agency to search certain designated premises and seize specific categories of items or documents. Generally, the requesting agency is required to establish that probable cause exists that evidence of a crime will be located. The warrant is authorized based on information contained in an affidavit submitted by a law enforcement officer.

When a search warrant is served, it is important that everyone present remain calm. Every employee should know that a search warrant is not usually an open-ended demand. Instead, it gives the law enforcement agents the right to enter the premises, search, and seize only certain items or documents. A search warrant also does not compel testimony.

When presented with a search warrant, an organization should consider taking the following steps:

- Call the financial organization's in-house or outside legal counsel and/or designated officer in charge of security, risk management, or a similar business area.
- Review the warrant to understand its scope.
- Ask for and obtain a copy of the warrant.
- Ask for a copy of the affidavit that supports the search warrant. The agents are not obligated to provide a copy of the affidavit; however, when a financial organization is allowed to review the affidavit, it can learn more about the purpose of the investigation.
- Remain present while the agents make an inventory of all items they seize and remove from the premises and keep track of the records taken by the agents.
- Ask for a copy of law enforcement's inventory of what it has seized.
- Document the names and agency affiliations of the agents who conduct the search.

Documents and computer records that are protected by the attorney-client and other legal privileges should be so marked and retained separately from general records. Privileged records should be stored in an area (e.g., a cabinet) labeled "Attorney-Client Privilege."

If law enforcement agents want to seize privileged records, organization representatives may object and suggest, as an alternative, that the records be given to the court for safekeeping. All employees should be trained on how to behave in a search, and one person should be designated to communicate with the agents.

Orders to restrain or freeze accounts or assets

When a law enforcement agency or prosecutor obtains a court order to freeze an account or prevent funds from being withdrawn or moved, the organization should obtain a copy of the order and make every effort to comply. Generally, such an order is obtained based on a sworn affidavit, which is sometimes included with the order. If the affidavit is not part of the order, the financial organization can ask to see the affidavit, which should provide clues as to why a customer's information is being requested. Whether law enforcement authorities are obligated to provide the affidavit depends on each country's laws and regulations. In some jurisdictions, freezing orders can also be executed by seizure warrant.

National security letters

National Security Letters (NSLs) are authorized by four federal statutes: the USA PATRIOT Act, Electronic Communications Privacy Act, National Security Act, and Fair Credit and Reporting Act. However, several amendments were added to the USA PATRIOT Act and the USA PATRIOT Act Reauthorization of 2006. These amendments significantly reduced the standards required to issue an NSL and expanded the utilization NSLs by the FBI and other federal agencies in limited circumstances when counterintelligence and counterterrorism investigations are being conducted.

The most common type of NSLs can be issued directly by the FBI leadership including the director, assistant director and special agents in charge. An NSL is a written investigative demand requiring third-party businesses, such as credit reporting agencies, telecommunications/internet service providers, and financial institutions, to provide a broad range of data and information on investigation targets, including telephone and electronic communications records, credit report information, and financial records

The NSL process is secret and does not require a judge's approval or other judicial oversight. Third-party businesses are not permitted to disclose the

receipt of an NSL (i.e., gag order). Pursuant to 12 USC 3414(a)(3) and (5)(D), no bank, officer, employee, or agent of the institution can disclose to any person that a government authority or the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL.

Keeping records

Proper recordkeeping is a requirement, and it can help protect a financial organization from regulatory findings. Records that must be kept include CDD information and EDD records. You must also keep information about suspicious activity reports made to the authorities and internally reported suspicious activity that did not require a report to the authorities. Finally, keep records that describe your internal AML controls and your training records for all relevant staff.

Sources of investigations (Case example: Preserving subpoenaed audio recordings)

In September 2020, the US Commodity Futures Trading Commission (CFTC) announced that it settled charges against Citibank and its affiliates, Citigroup Energy Inc. and Citigroup Global Markets. Citibank failed to preserve audio recordings that were subject to a hold notice in connection with a subpoena sent by the CFTC's Division of Enforcement in December 2017. Citibank admitted that more than 2.77 million audio recordings were deleted due to a flaw in its system, including files responsive to the subpoena that should have been preserved. The Citibank entities agreed to pay a US$4.5 million fine.

CFTC determined that, from at least 2014 through at least November 2018, Citibank entities violated CFTC regulation 166.3: Failure to supervise. According to the regulation, records subject to subpoena should be segregated and stored safely. Senior management should ensure that adequate systems and staff are in place to meet legal and regulatory requirements. Any recordkeeping and regulatory deficiencies should be escalated to senior management and addressed in a timely manner. In addition, remedial action plans should be required, implemented, and tracked for system deficiencies.

In 2014, Citibank determined that the system used to preserve audio recordings was not reliable for addressing legal holds to meet recordkeeping requirements and regulatory requests. Citibank implemented a stopgap measure to preserve audio recordings indefinitely. The audio recordings would be preserved as long as there was sufficient storage space. The system reached the storage threshold in October 2018 and automatically began deleting older recordings, including recordings subject to a December 2017 subpoena. The subpoena department should have sent legal hold notices to the applicable parties and segregated and preserved the responsive records. This did not occur. Further, despite being notified of the problem, Citibank did not take timely and adequate steps to mitigate the associated risks.

Citibank's failures, which led to deleting audio recordings subpoenaed by the CFTC Division of Enforcement staff, included:

- Failed to adequately staff the department responsible for the oversight of audio recording preservation
- Failed to adequately train staff to understand and recognize the risks of deleting audio files based on first-in, first-out settings
- Failed to fully document system changes and ensure adequate procedures were in place for the system
- Failed to preserve audio recordings through system backups
- Failed to escalate the system weaknesses to Citibank management, the legal department, or any other compliance department

Key takeaways

- Records subject to subpoena should be segregated and stored safely.
- Senior management should ensure adequate systems and sufficient staff are in place to meet legal and regulatory requirements
- Recordkeeping and regulatory deficiencies should be escalated to senior management and addressed in a timely manner
- Remedial action plans should be required, implemented, and tracked for system deficiencies

Sources of investigations (Case example: Acting on seizure warrants)

Regulators assessed a civil money penalty against a midsize regional bank for failing to maintain an effective anti-money laundering program. The regulators determined that Midsize failed to detect suspicious activity related to legal orders and failed to file timely suspicious activity reports (SARs). Over US$100 million in criminal proceeds from a trade-based money laundering scheme was processed through the institution over a four-year period.

Additionally, despite receiving a seizure warrant from law enforcement, the bank failed to freeze US$1.25 million in funds from the suspect account. The bank was ordered to pay a US$10 million civil money penalty and agreed to a US$1.25 million forfeiture.

The bank required its legal department to process all legal orders, including subpoenas, keep-open letters, and seizure warrants. However, the legal department did not establish a formal process or document written policies for reporting legal orders related to bank customers to the AML department.

The AML department also did not adopt policies requiring the review of subpoenas, keep-open letters, and seizure warrants to determine if the underlying account activity was suspicious. Accordingly, it failed to review hundreds of accounts that were subject to legal orders for suspicious activities. It also failed to file timely SARs. In one case, the AML department failed to review an account subject to multiple subpoenas which resulted in over US$100 million in suspicious transactions. The AML department was unaware the account records had been subpoenaed.

Law enforcement served a seizure warrant for US$1.5 million in funds remaining in the account. However, the bank allowed an additional US$5 million in funds transfers to be processed through the account. Eventually, the remaining balance was US$250,000. The legal department failed to freeze the funds due to backlogs, and the AML department had not been informed of the seizure warrant.

Ultimately, the bank agreed to forfeit US$1.25 million related to the funds released. The regulators ordered the bank to pay a US$10 million civil money penalty.

Key takeaways

- Financial organizations must implement policies and procedures to appropriately respond to legal orders, including timely processing of seizure warrants.
- Effective communication among departments within financial organizations is critical to ensure that suspicious activities are reported to the AML department.
- The timely filing of SARs is an important element of effective AML programs.

Conducting the Investigation

Several key actions are required to conduct an effective financial investigation into potential suspicious activity, including:

- Reviewing internal transactions, including value and volume, information obtained from the customer, and other relevant internal documentation
- Determining whether the activity is expected for the customer
- Identifying and reviewing external information to understand the customer, related entities, and relevant media
- Contacting business line employees who are responsible for the account relationship
- Generating a written report that documents relevant findings

A financial investigator's main objective is to track the movement of money, whether through a bank, broker-dealer, money services business, casino, or other financial organization. Financial organizations have access to a wealth of information, because they are in the business of taking in, paying out, accounting for, and recording the movement of money. For example, banks maintain signature cards, which are collected at the opening of an account, account statements, deposit tickets, checks and withdrawal items, and credit and debit memorandums. Financial organizations also keep records on loans, cashier's checks, certified checks, traveler's checks, and money orders. They exchange currency, cash third-party checks, and conduct wire transfers, as

do most MSBs. Financial organizations also keep safe deposit boxes and issue credit cards. Online-based financial organizations maintain login activity logs, IP addresses, and geographical location information.

Often, financial organizations are required to keep records of customer accounts for five years, such as in the EU, US, and Canada. Although that rule might vary in different countries, it is important for compliance officers at financial organizations to be aware of these legal requirements. Account records and records of other nonaccount activities can be essential to tracking possible money laundering. Other financial organizations keep similar records of transactions and the ability to exert control over an account, such as the ability to trade stocks in a brokerage account.

With all the information financial organizations are privy to, it is important for them to develop and maintain policies and procedures regarding financial investigations. Typically, financial organizations identify the procedural steps required, the information needed to complete the investigation, and any recommended next steps.

Following are two examples of the steps in a financial investigation:

1. An investigation is initiated after a branch teller identifies a new customer who conducted large cash deposits at three different branches on consecutive days just below the statutory cash-reporting threshold. Subsequently, the customer wired 95 percent of the funds to an unrelated individual located in a high-risk jurisdiction that is known as a gateway for narcotics traffickers. According to the financial organization's investigation policies and procedures, the following must be done: Conduct a documented review of the customers' accounts for one year, including all transactions, KYC information, and social media searches for any relevant negative media. The report must analyze the information reviewed, determine whether or not a SAR should be filed, and take any additional remedial measures.
2. An investigation results from a transaction monitoring alert that identified large, round-dollar wire transfers to a commercial customer from import/export companies with generic names located in high-risk jurisdictions. The KYC review indicated the customer was engaged in furniture sales through several retail locations. Further, it identified a high volume of incoming check and credit transactions and no incoming wire transfers; however, the customer originated wire transfers to low-risk

jurisdictions to purchase the furniture. This investigation led to contacting the relationship manager for information about the customer's activity to assist with explaining the deviation. If unexplained, the next step in the investigation would be to determine whether such activity warranted a SAR filing.

Utilizing the internet when conducting financial investigations

An effective investigation requires that information be sourced both from the information held by the financial organizations and from external sources. Care should be taken to ensure that the information found is reliable and verifiable, and the assistance of external specialists is sought if necessary. It is critical to be confident about the soundness of the information relied upon during an investigation, especially when it could be the deciding factor in closing an account or terminating a business relationship.

The internet is often used to source information as part of internal investigations. A focused approach to searching reliable and reputable sources can provide useful third-party information and additional context to the files held by financial organizations. Combined with a review of internal documents and records, internet sources can help provide a complete understanding of whether further steps are needed to mitigate possible financial crime risks associated with the customer.

Conducting research on the internet is most effective when there is a clear understanding of what online sources are considered reliable. For example, social media sites such as Facebook and LinkedIn can be useful to verify some information, but blogs and comments posted on these sites might not prove to be reliable sources about an individual's reputation. Independent websites maintained by independent standards bodies (e.g., FATF, Wolfsberg, and OECD) and supervisory authorities (e.g., national and state-level regulators, corporate registrars, electoral rolls, and registration lists) can provide valuable information concerning regulatory status, sanctions, fines, business activities, and broader commercial activities of the party under investigation. Furthermore, these sources are considered to have a high degree of reliability.

In some countries, court lists, decisions rendered by courts, magistrates, administrative tribunals, and professional oversight bodies with disciplinary powers (e.g., law societies) can be useful sources of information.

When using the internet to glean customer reputation information, care must be taken when researching news and quasi-news websites. Steps should always be taken to verify, from more than one source, the accuracy of negative news articles to reduce the risk of relying solely on a writer's opinion. Journalists have their own biases, as do their employers, and these biases can subtly find their way into news articles. In addition, in countries where freedom of speech and press are not well established, journalists are not always free to write exactly what they would like. This often takes the form of prominently publicizing negative news about someone who is not in favor with the government (including what could be politically motivated criminal or civil charges) or downplaying negative news about someone in favor with the government. Not all media is corrupt, but sometimes the source has as much at stake as the subject of the news. This is why investigators must take a close look at the source of the news as well as the news itself, and why getting multiple sources is important to ensure a complete understanding of the story. Some sources might have limited parts of the whole story, which only is revealed when the investigator has additional pieces of information.

When dealing with a country or region that is known to have tighter controls on what is published on the internet and to restrict the amount of information that is publicly accessible, it may be necessary to seek additional assistance. Particularly when dealing with a valuable customer that justifies the additional expense, an organization can retain the services of a vendor with expertise in this area to verify whether serious adverse information about a customer is in fact supported by independent sources.

Tips on searching the internet

Before searching the internet, the investigator should prepare a plan, focusing on the topics under investigation and the types of information needed. This will ensure that the work is undertaken in an efficient and focused manner, with the relevant records retained (e.g., screen capture or downloads due to the risk of website changes).

The investigator should start with a metasearch using several different search engines and then move to specific search engines with different capabilities. From the metasearch, the investigator can start narrowing the parameters using keywords. The plan devised in advance will help the investigator select the keywords and areas where greater focus should be applied. For example, if a customer's transaction activity has raised concerns, the search could

begin with the customer's personal and professional background and then focus on the nature of the commercial activities she has been undertaking. This will assist the investigator in assessing whether the transactions appear to be consistent with the reasons given by the customer for opening the account and the expected commercial activity she proposed to use it for.

There are high-quality tutorials on the web for individuals who want to improve their search skills. There are also sites that identify search engines for professional researchers. The easiest and most effective way to improve your web-searching skills is to read the Help pages of major search engines and to practice with their advanced features.

Some tips on search engines include:

- Using multiple search engines is effective because no single engine covers the entire web.
- If you are searching in a foreign country, use a local search engine.
- Use metasearch engines.

  An additional step is to access a commercial database. Although these databases require the payment of a fee, public record aggregators can be cost-effective, because they cross-reference an enormous number of records. Moreover, they can include certain personally identifiable information, such as date of birth and government identification number, which might not be located on the internet.

  Search scenario: Too much money. Consider the case of a gas station owner who deposits US$50,000 in cash per week. Is this money laundering? Would simply searching the owner's name on Google be considered sufficient due diligence? A better approach would be to search how much cash gas stations of that size and location typically deposited. This leads to a very different line of inquiry. Internet sources might reveal sources such as marketing studies, commercial valuation sites, and businesses for sale that could provide useful clues about the cash flow of comparable gas stations.

  The internet might also reveal useful information about the area in which the gas station is located, such as population statistics, income levels, ethnicity, and crime rates. Is it located on a commuting corridor? Are there

competitors nearby? Does it have a car wash or a convenience store attached?

By comparing the business with others and examining the context, it becomes possible to argue that there is "…a high level of cash deposits atypical of the expected business profile"—a classic indicator of money laundering.

Search scenario: Unknown business. A bank client was depositing large amounts of cash in his personal account. The bank suspected that its client was operating an unlicensed money remittance service out of the back of his restaurant. It was about to file a SAR when the bank realized that it was missing a key piece of information: the name of the client's restaurant. How did the bank solve the mystery? It began by assuming that the client's restaurant was near the bank. Using a simple online telephone directory, the bank was able to generate a list of all the restaurants within one mile of the bank.

But which one belonged to the client? The bank needed a way to search incorporation records for each of the businesses that it had identified. Not wanting to use a commercial service, it went to a free online public records provider. Clicking on the jurisdiction and then the link for corporations led the bank to the right government department, where it input the name of each one of the area restaurants until it found one with its customer listed as a director.

This case provides a useful example of the benefits of starting an investigation and then focusing on more specific areas to gain a complete understanding of the customer being investigated.

Search scenario: Unusual bank account activity. What technical skills are useful for KYC and due diligence? The following simple scenario can be used to consider how to approach an investigation. You are asked to research a customer named Cynthia Jenkins in Albuquerque, New Mexico. Transaction monitoring raised an alert that Cynthia appeared to be using her account in a way that was inconsistent with what was expected when she first opened the account—or maybe the account had been dormant for some time and had suddenly reactivated. Transaction monitoring showed that Cynthia's account had received a significant number of wire transfers from different parties in the past two weeks. Each transfer was

for US$9,900. When Cynthia first opened the account, she stated that it was for “household expenses.”

Your first step might be to confirm Cynthia’s identity and search the internet to determine whether the use of the account appears to be legitimate, for example:

- Is she listed in the telephone directory or on the electoral roll?
- Where does Cynthia live? Is there any evidence that the property is used for any commercial activity that could justify the payments received?
- Is she mentioned in any other public records? Try a public records search engine.
- What information does she provide on social media about her occupation, location, and other aspects of her life?
- Is there evidence that someone could be misusing Cynthia’s account? For example, is she elderly or possibly deceased? Could this be a case of identity theft? Imposters often use the Social Security numbers of deceased people. In the United States, it is possible to check the Social Security Death Index by searching for “Social Security Death Index.”

Information obtained from internet searches should be complimented by internal documents and records held by the financial organization. For example, who sent the transfers? From what banks? Do the transfers indicate why the monies were paid? Is it possible to check the internet to see whether there is any information about the payers?

Conducting the investigation (Case example: Utilizing the internet when conducting financial investigations)

Easy Cash Ltd. is a money services business (MSB) that has been a customer of XYZ Bank Corp for seven months. During customer onboarding, Easy Cash advised XYZ Bank that its customers would come from Europe and that it would conduct an estimated 10 to 20 transactions on the account each month.

During the regular transaction monitoring of its customers, XYZ Bank identified possible anomalies with the Easy Cash transactions and initiated an investigation.

The investigator reviewed Easy Cash's KYC and transaction history. It also used open-source intelligence (OSINT), i.e., information obtained from data that is publicly available. OSINT is often used in financial crime investigations and KYC processes to better understand key information related to customers and their activities. It is often used in conjunction with internal and closed sources and helps to analyze different aspects of cases using primary and secondary information related to the investigation that could corroborate or disprove concerns and information.

OSINT involves searching through a large variety of online sources, such as social media, news sites, public registries, and websites, in a structured and logical manner. It can involve the use of basic search strings to find data using key terms or delve into more complex techniques involving artificial intelligence-driven automation capabilities and external platforms to compile and analyze data.

The investigator started with a web search of the name of the customer and its ultimate beneficial owner (UBO) for potential adverse media. She also searched the names of senders and recipients of transactions using key words, for example, "money laundering" or "crime," and Boolean operators such as "AND" or "OR." The investigator learned that one of the recipients of several transactions was mentioned in multiple reliable media sources as having ties to the Italian Mafia and using Italian restaurants for laundering money.

She also accessed the home page of the customer and businesses associated with the UBO. On the home page of Easy Cash, the investigator discovered that the company was promoting its money transfer services in the Middle East and East Africa and downplaying the need to provide KYC. She also discovered that Easy Cash had a branch in Turkey. Because some of the home page content was written in a language the investigator did not speak, she used an online translation tool and identified it as Farsi, the language spoken in Iran. The Farsi content promoted the services of Easy Cash to transfer funds in various currencies, including US dollars. The investigator also used an online map service to research the address of the Turkish branch and discovered that it was located in a city near the Iranian border.

XYZ Bank quickly took steps to freeze and later close the account with Easy Cash once it notified the finance intelligence unit (FIU) of its findings.

Key takeaways

- OSINT is an effective tool for investigations.
- OSINT uses various search engines and conducts key word searches.
- Boolean operators enhance the effectiveness of an internet search.
- Customers' home pages can provide important information.
- Online translation services can help you utilize foreign websites in investigations.
- Online map applications can verify locations and determine what is physically near that location.
- Report to your FIU when you suspect a customer is engaged in money laundering.

SAR Decision-Making Process

The decision of whether or not to file a SAR often involves weighing the aggravating and mitigating factors arising from the research conducted during the investigative process. Financial organizations should draft procedures that document the factors to consider when determining whether a SAR filing is appropriate. Properly trained personnel in charge of investigating and reporting suspicious activities should have a clear and concise procedure for escalating their findings to a compliance officer, manager, or other staff member with authority to make the filing decision. The final decision should be documented and supported by the reasoning that was used to make the determination. Often, the reason not to file an SAR is as important as the reason to file an SAR.

After the decision to file has been made, the organization should report the activity to its regulatory agency, law enforcement, or both, as defined by the applicable regulations within its jurisdiction. Many jurisdictions require SARs to be filed within a specific number of days following the discovery of potentially suspicious activity.

In many jurisdictions, it is a requirement to report certain information regarding SARs to senior management and/or the board of directors. This information could be limited to the number of reports filed, the dollar amounts involved, and significant trends observed by compliance personnel. In some cases, if the activity presents a significant or potentially ongoing risk to the organization, the leaders should be notified so that high-level decisions can be made regarding potential changes to systems, staffing, products, services, or specific relationships maintained by the organization.

Filing a SAR

The decision to file a SAR should be the result of an accumulation of aggravating factors and a lack of mitigating factors, in combination with the knowledge of what is expected activity for the organization's customer base, product offerings, and geographical area of service. The SAR filing should include the details of the suspicious activity and the related demographics, as well as the reasons the organization finds the activity suspicious. The recipient of the SAR does not have the intimate knowledge of what is expected activity for a particular organizations, clients, and products, and will only benefit from

the inclusion of this information. In addition, any known typologies identified as part of the review should be included in the filing as well.

If, following the investigation, the organization decides that it should file an SAR, it should notify the investigators or prosecutors as soon as possible. However, this might not be practical in certain jurisdictions due to the continuous nature of the SAR process and the volume of reports filed by the reporting organization. The establishment of a filing timeline in concert with country guidelines is critical to avoiding organizational penalties and fines. The failure to file timely reports is often cited in regulatory actions against financial organizations. The AML/CFT officer or designee should keep senior management and board members apprised of SAR filing metrics and any significant issues resulting from those filings, especially items that pose a regulatory or reputational risk to the organization.

Finally, the financial organization should maintain a record of the SAR and all supporting documentation. Under the BSA record-retention requirements, this information should be maintained for five years following the date the SAR was filed.

Quality assurance and control

All financial organizations are required to file timely and complete SARs, and the quality of the SARs can be an indication of the quality of a financial organization's AML/CFT program. Quality and consistency in the SAR decision-making process is critical to ensuring the appropriate level of oversight in the investigative process. A quality assurance (QA), or quality control (QC), review helps to ensure that SAR filings are internally consistent, the right decisions are being made, and high-priority issues are identified and escalated to leadership. A strong QA/QC process is also needed to ensure that SARs are completed according to all regulatory requirements. The larger the scale of the financial organization, its staff, and where it is located all have an impact on the QA/QC process. As a result, financial organizations that implement a QA/QC process should document the requirements and qualifications of QA/QC reviewers and regularly review the outcome of QA/QC reviews to assess the quality of staff, training requirements, and the general health of the program.

SAR filing oversight and escalation

An organization should have robust policies and procedures for documenting the appropriate oversight of the investigation process and regulatory reporting requirements. This should include specific actions to be taken, such as escalation to senior management in cases in which a customer-facing employee or individual in the AML/CFT chain of command is complicit or willfully blind to suspicious financial activities.

Failing to report SARs (Case example: Money laundering reporting officer)

Governments and regulators routinely enact laws and publish guidance to ensure that professionals report suspicious activity within various business functions in an effort to identify, manage, and mitigate money laundering and other financial crimes.

In June 2021, the UK updated guidance on prosecuting “failure to disclose” cases under section 330 of the Proceeds of Crime Act 2002. It is now legal to prosecute the offense of failing to report suspicious activity, even when the suspected money laundering activities have not yet been determined. The intention of the updated guidance is to encourage professionals to actively report any suspicious activity to the authorities; in the UK, this would be the UK financial intelligence unit (UKFIU). The money laundering reporting officer (MLRO), Bank Secrecy Act (BSA) officer, and other designated persons “report” or “sign” as the reporter to their FIU. The boards of financial organizations delegate such functions to these appropriately trained and experienced people. A conviction for failure to disclose information on suspected or determined money laundering activity can result in a five-year prison sentence.

In July 2021, Dominic Thorncroft was given an 18-month suspended prison sentence and ordered to do 250 hours of unpaid work at Southwark Crown Court, UK, for failing to alert the authorities to money laundering (i.e., not reporting SARs), breaching money laundering regulations, and retaining a wrongful credit.

Thorncroft was an MLRO for a money services business (MSB) and the former chair of the Association of UK Payment Institutions. In that capacity, he worked with lawmakers and financial regulators and provided AML advice and training.

An investigation by the Metropolitan Police found evidence linking Thorncroft to a 2014 investment fraud. Thorncroft had allowed his MSB to be used by fraudsters to transfer money to Hong Kong and mainland China. In addition, he knowingly transferred money to the fraudsters, despite the fact that one individual was subject to a serious crime prevention order, which should have stopped him from sending money overseas.

Investigators found that Thorncroft should have known or suspected that the money passing through his business's bank accounts was criminal property. Despite his substantial knowledge and expertise of money laundering, Thorncroft failed to alert the authorities to the suspicious activity and allowed it to continue.

It was noted in court that "Thorncroft did not commit the fraud himself. However, his actions have allowed £850,000 defrauded from 60 individuals to be dispersed across the world." Thorncroft promoted himself as an anti-money laundering expert, but he did not follow the standards he set for others. When his business was clearly being used to launder criminal property, he failed to follow his own advice and report what was happening to the authorities.

Key takeaways

- Designated persons must ensure that suspicious activity is identified and reported through SARs to FIUs, to protect potential crime victims, their firms, and themselves.
- Designated persons must be held accountable, as they have a higher level of knowledge and thus responsibility compared with others in businesses.

Failing to report SARs (Case example: Deutsche Bank)

Suspicious activity reports (SARs) are routinely described by law enforcement as the “lifeblood” of financial investigations. They contain intelligence related to criminal financing and useful supporting contextual information. SARs can be the catalyst for new investigations or a vital “piece of the puzzle” for an existing investigation. Law enforcement officers rely on designated individuals such as money laundering reporting officers (MLROs) and Bank Secrecy Act (BSA) officers to identify and report suspicious behavior in a timely manner.

To fight financial crime, organizations must know the current reporting laws and regulations and take responsibility for reporting suspicious activity. This will protect the individual designated officers and the organization. The person who detects the suspicious activity is responsible for reporting it internally for further development to establish whether the activity is suspicious. The MLROs, BSA officer, or other designated officer “reports” or “signs” as the reporter to the financial intelligence unit (FIU). At a higher level, the board must ensure that the right people, technology, and processes are in place to meet the reporting requirement. Reporting is genuinely a collective responsibility but reporting to the FIU is the responsibility of the MLRO, BSA officer, or designated officer.

People working in regulated sectors must exercise a greater level of diligence by identifying and reporting any red flags that might indicate suspicious activity. Regulators have taken action against numerous organizations for failure to report suspicious activity.

In October 2020, Deutsche Bank received a €13.5 million administrative fine for failing to submit SARs in a timely fashion. Deutsche Bank allegedly failed to disclose more than one million suspicious money transfers with Danske Bank Estonia, for which Deutsche Bank was the correspondent bank.

The money transfers occurred over a five-year period after a whistleblower at Danske Bank flagged them as suspicious transactions. German prosecutors launched an investigation to determine whether Deutsche Bank employees had sanctioned these transactions and subsequently attempted to cover them up. Deutsche Bank withdrew from its position as a correspondent bank for Danske Bank Estonia over increasing concerns about potential misconduct

by Danske Bank and launched two internal investigations into the matter under the scrutiny of US regulators.

Frankfurt prosecutors cleared Deutsche Bank of money laundering, but found that, between 2010 and 2015, Deutsche Bank failed to send timely alerts of potentially suspicious transactions to law enforcement authorities on 627 occasions. For each of these failures, Deutsche Bank was fined between €12,500 and €30,000.

Key takeaways

- Failure to report suspicious transactions can result in fines and other penalties.
- People working in regulated sectors must exercise a greater level of diligence by identifying and reporting any red flags that trigger suspicion.
- Financial organizations are required to report suspicious activity by filing SARs with FIUs.

Closing the Account

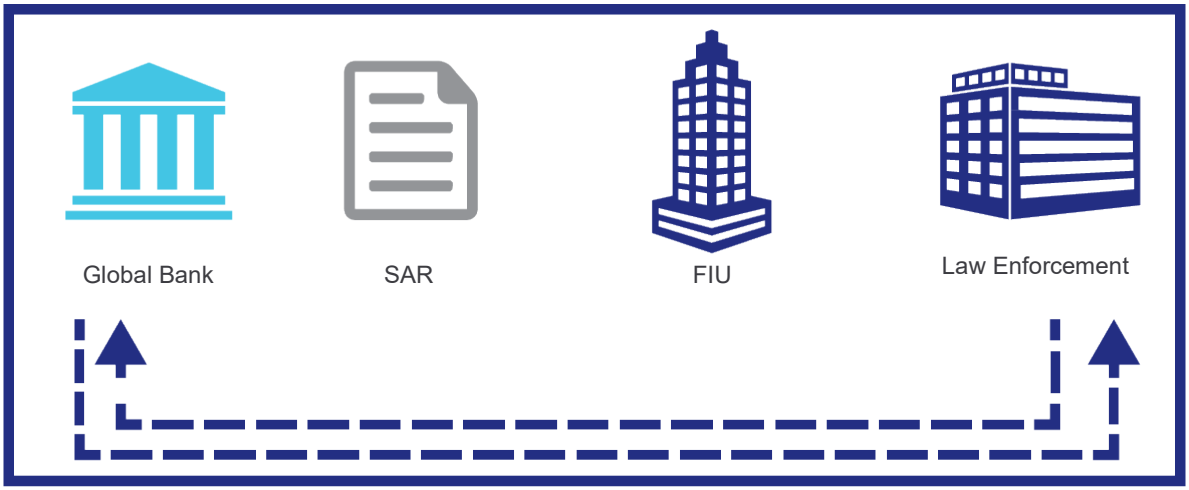
Based on its internal investigation, the financial organization should independently determine whether to close the account in issue. Following are important factors the organization should consider:

- The legal basis for closing an account
- The organization's stated policies and procedures for closing an account, which might include an automatic closure recommendation following a specified number of SAR filings
- The seriousness of the underlying conduct; that is, if the conduct rises to the level of seriousness at which it would typically be closed, the organization should consider closing it
- The reputational risk to the organization posed by maintaining the account
- Correspondence with law enforcement and requests from law enforcement to either cancel or maintain the account

Communicating with Law Enforcement on SARs

When an organization files an SAR, the details of that filing might warrant additional law enforcement notification. SARs represent financial intelligence to a country's FIU; depending on the volume of reports filed in a given country, a report worthy of priority attention could be lost in the large number of reports filed. Following the filing of the SAR, the responsible compliance officer or designee can contact a specific law enforcement division to notify it of the recent filing and make it aware of activity relevant to its area of coverage or geographical location. Moreover, a law enforcement agent can contact the financial organization that filed the SAR to seek the underlying information used in the investigation that resulted in the SAR. Therefore, it is critical that each organization develop its own policies and procedures for communicating with law enforcement regarding SARs.

Communicating with Law Enforcement on STRs Example



Investigations Initiated by Law Enforcement

Law enforcement agencies may initiate investigations against a financial organization or contact financial organizations in the context of an investigation involving a customer. Steps that law enforcement agencies can take when conducting a money laundering investigation include:

- **Follow the money:** When a law enforcement agency is aware of where laundered money originated or where it ended, it is appropriate for the agency to attempt to bring the two ends together and compile a complete understanding of the flow of the funds.
- **Leverage the financial knowledge and due diligence information contained in financial organizations:** Through information sharing and transactional reviews, a financial organization can assist law enforcement in identifying the originating and ultimate destination of a subject's funds. Furthermore, the supporting documentation that was used to create a SAR or CDD file may be used as evidence, whereas actual SARs may not be in many jurisdictions.
- **Identify the unlawful activity:** Most countries define money laundering in terms of predicate offenses or specified unlawful activities. These activities are usually very extensive and include many felony crimes, such as bribery, extortion, racketeering, narcotics trafficking, and human trafficking. For a money laundering case to result in a conviction, prosecutors need to establish the flow of money and the existence of a predicate offense.
- **Review databases:** FIU databases and commercial databases can provide very useful and extensive financial information and provide leads regarding which financial organizations to ask for assistance. Also, records, such as Social Security information in the United States (i.e., tax-related information), can be used to further identify subjects.
- **Review public records:** Court records, corporate filings, and credit reports can provide useful background information.

- **Review licensing and registration files:** Files, such as records held by motor vehicle departments and other registration databases, can provide background information and useful leads.
- **Analyze the financial transactions and account activity of the target:** Look for the typical and expected transactions of the individual or entity based on self-disclosures, income, and typical flows of funds by similarly situated people. Financial organizations might be able to assist in identifying these items. If the transactions are outside of the norm or stated level of activity, analyze where the additional funds originated and the composition of the unusual activity.
- **Review SARs that might involve any potential individual linked to the target, transactions, or activity.**
- In cross-border cases, **seek international assistance.**

Decision to Prosecute a Financial Organization for Money Laundering Violations

- When considering whether—or to what extent—to bring a case against an organization involving money laundering-related charges, prosecutors consider many factors, such as: The organization has a criminal history.
- The organization has cooperated with the investigation.
- The organization discovered and self-reported the money laundering-related issues.
- The organization has a comprehensive and effective AML/CFT program.
- The organization has taken timely and effective remedial action.
- There are civil remedies available that can serve as punishment.
- Deterring wrongdoing by others is needed and will be served by a prosecution.
- Advice and recommendations from regulatory agencies and/or the FIU for the jurisdiction is available.

Assuming the case is not simple or egregious, the decision to prosecute is frequently determined by what the prosecutors believe was the intent of the organization when it undertook the action in question.

Responding to a Law Enforcement Investigation against a Financial Organization

When a financial organization is confronted with a law enforcement investigation or a regulatory agency, it should respond quickly and completely to all requests. Failure to do so could cause unnecessary risk or damage to the organization. If a request is overly broad or unduly intrusive, the organization can attempt to narrow the request or even seek to contest the request, or portions of the request, in court. However, under no circumstances should an organization ignore or delay responding to a law enforcement inquiry or request for documents.

Upon receipt of a law enforcement inquiry, the financial organization needs to inform the appropriate senior management and designate an individual to respond to all law enforcement requests, monitor the progress of the investigation, and keep senior management, including the board of directors, informed of the nature and progress of the investigation. Reports and other information about an investigation should not be provided to any employees, officers, or directors of the organization who might be implicated in the investigation.

The financial organization should consider retaining qualified, experienced legal counsel. Such counsel can guide the organization through the inquiry, contest requests that are perceived as improper, and assist in negotiating settlements, when necessary.

As described below, when an organization receives a subpoena, search warrant, or similar law enforcement demand, or becomes aware of a government-related investigation involving the organization, it should conduct an inquiry of its own to determine the underlying facts, the organization's exposure, and what steps, if any, the organization should take.

Monitoring a Law Enforcement Investigation against a Financial Organization

Financial organizations should ensure that all grand jury subpoenas and other information requests from government agencies are reviewed by senior management and an investigations group or legal counsel to determine how best to respond to the inquiry and whether the inquiry or the underlying activity might pose a risk to the organization. In addition, the organization should maintain centralized control over all requests and responses to ensure that it responds to requests on a complete and timely basis and maintains a complete record of information provided. This centralized record will also assist in the organization's internal investigation.

Vital information can be found in a wide variety of document types, including internal memos, transactional documents, calendars, emails, financial records, travel records, phone logs, signature cards, deposit tickets, checks, withdrawal items, credit and debit memoranda, and loan records. Thus, the organization must ensure that relevant documents are not altered, lost, or destroyed and that all employees are advised of this fact. This can be done by a memo sent to all relevant employees. However, if there is concern that such a memo might prompt a particular employee to alter or destroy documents, that situation must be managed separately.

The organization should also address its document destruction policy to ensure that no documents are destroyed pursuant to that policy during the investigation. It would not be a serious concern if documents relevant to a government investigation were destroyed pursuant to a legitimate policy and prior to obtaining knowledge of the investigation or receiving a subpoena. It could, however, be a serious concern if such documents were destroyed for any reason (even pursuant to a legitimate policy) once the organization was notified about an investigation—even if no subpoena had yet been received.

The organization should ensure the integrity of original documents, while at the same time minimizing disruption to the organization's business. It must ensure that an appropriate system is in place to organize, maintain, number, secure, copy, and prepare the documents for production to the government (or to the opposing party in civil litigation). The documents should be listed in an index so that they can be found when needed.

A detailed privilege log should also be created as the documents are gathered, and privileged documents should be separated from other documents to help avoid inadvertent disclosure.

Cooperating with Law Enforcement During an Investigation against a Financial Organization

Providing investigators with the information they need to reach an investigative conclusion might be the most effective way to terminate an investigation before it has a devastating effect on the resources and reputation of an organization. Cooperation could include making employees, including corporate officers, available for interviews, and producing documents without the requirement of a subpoena. It could also include a voluntary disclosure by providing investigators with any report written by counsel regarding the subject under investigation.

The organization should make every effort to maintain a positive relationship with the investigators and prosecutors. At a minimum, a positive working relationship will help the organization conduct an effective parallel internal investigation and thereby position the organization to respond more effectively to investigative and prosecutorial inquiries.

It is also important for the organization to try to learn how the investigators and prosecutors view the facts. If they are incorrect about some of the facts, the organization will have an opportunity to correct them. At a minimum, if the organization is aware of the investigators' and prosecutors' concerns, it will be in a better position to respond to them.

Obtaining Counsel for an Investigation against a Financial Organization

Retaining counsel

In particularly large, important, or serious investigations, it might be appropriate for the organization to retain legal counsel to assist in responding to the investigation or advising the organization during the course of the investigation. Many financial organizations, such as large banks and securities dealers, have legal counsel on their staff. But many other organizations, such as small MSBs, do not ordinarily have legal counsel on their payroll. In either case, it is recommended that organizations hire or consult with experienced external legal counsel when confronted with a government investigation of the organization itself. If the organization is actually facing imminent criminal prosecution or indictment, it needs an experienced attorney who specializes in defending financial organizations in these matters.

Using in-house counsel will, of course, cost less, and in-house counsel will start out with a better knowledge of the organization and its personnel, policies, and procedures. However, if the conduct under investigation could involve or lead to a criminal investigation or indictment, outside counsel could be more appropriate.

If the organization determines that it is appropriate to involve counsel, in-house or external, it should take appropriate measures to ensure that the counsel is sufficiently experienced and knowledgeable regarding the factual and legal issues involved. In addition, the organization should determine the nature and scope of the role of counsel and ensure that senior management is aware of and supports the involvement of counsel.

Attorney-client privilege applied to entities and individuals

In an internal investigation, all parties should be aware that attorneys for the organization represent the entity and not its employees. Counsel should understand these issues and conduct the internal investigation accordingly. Work product and communications might be protected under attorney-client privilege. There can be serious consequences when the interests of an entity

and its employees diverge or conflict, and when an employee implicates the employer, or vice versa. In such cases, separate counsel could be required.

Dissemination of a written report by counsel

If counsel for the organization prepares a written report of an investigation, the organization should take steps to not inadvertently waive the attorney-client privilege by distributing the report to people who should not receive it. Every page of the report should contain a statement that it is confidential and subject to the attorney-client privilege and work-product privilege.

Copies of the report should be numbered, and a list of people who are given copies to read it should be maintained. After a specific period of time, all copies should be returned. Individuals who receive the report should be instructed not to make notes on their copies. All copies should be maintained in a file separate from regular organization files to maintain the highest level of protection.

Notices to Employees as a Result of an Investigation against a Financial Organization

In investigations conducted by the government, employees should be informed of the investigation and instructed not to directly produce corporate documents. Rather, they should inform senior management or counsel of all requests for documentation and provide the documents to them for production. In that way, the organization knows what is being requested and what has been produced. In addition, the organization can determine what, if any, requests should be contested. The same procedure should be followed with requests for employee interviews.

Interviewing Employees as a Result of a Law Enforcement Investigation against a Financial Organization

In addition to securing and reviewing all relevant documentation, it is important to interview all knowledgeable employees. These employees should be interviewed as soon as possible so that their memories are fresh, and they can direct management or counsel to relevant documents and people on a timely basis.

In addition, the organization, usually counsel, should prepare employees who expect to be interviewed by law enforcement investigators and debrief them after their interviews. The former will help the employee understand how to handle the process, and the latter will assist the organization in better understanding the scope and direction of the government investigation. All requests for employee interviews by law enforcement investigators should go through a single person or centralized location.

Most employees are not accustomed to or comfortable with being interviewed—either by law enforcement investigators or counsel for the organization. Therefore, care should be taken to put them at ease to the extent possible.

It is also helpful for interviews to be as noncontentious as possible. Background and open-ended questions should be used at the beginning of the interview, together with a nonconfrontational review of documents. When necessary, more contentious questions should be delayed to the end of the interview.

Media Relations

The importance of public and media relations in defending an organization should not be overlooked. Public perception is vital to an organization's success in maintaining public trust. If the facts are not on the institution's side, "no comment" might be the best response it can offer. Misleading or false statements that attempt to indicate that the organization has no problems and has done nothing wrong can worsen the situation. When such statements are made by a publicly traded company, they can invite additional scrutiny by regulatory and law enforcement agencies.

Media relations (Case example: Cooperation with regulatory authorities to reduce fine)

In October 2021, the UK's Financial Conduct Authority (FCA) fined Credit Suisse bank over £147 million for serious anti-financial crime (AFC) due diligence failures related to loans that it provided to the Republic of Mozambique. As part of its agreement, the bank also agreed to forgive US$200 million of the corrupt debt, which created economic harm and a debt crisis for Mozambique.

In its formal statement, the FCA emphasized that, although Credit Suisse was aware that the corruption risk of government officials was high, the bank failed to properly manage the associated financial crime risks within its emerging markets business.

Between late 2012 and early 2016, Credit Suisse was given information that should have revealed the unacceptably high risk of bribery associated with the loans and bond exchange the bank provided to a Mozambique government-sponsored project. To secure more favorable terms for the loans, kickbacks estimated to be over US$50 million were paid to members of a Credit Suisse unit who took steps to conceal these from the bank's senior management. The FCA concluded that there was insufficient challenge, scrutiny, and investigation into significant red flags concerning the transactions, which included bribery and corruption concerns over the contractor.

Credit Suisse agreed to pay US$475 million in fines and penalties as part of a coordinated international resolution with criminal and civil authorities in the United States, Switzerland, and the United Kingdom. The resolution included a deferred prosecution agreement with the US Department of Justice. The FCA stated that the debt relief provided to the Republic of Mozambique was taken into account when determining the fine. In addition, the bank was awarded a 30% discount in the overall penalty due to their cooperation. Without this cooperation, a significantly larger penalty would have been imposed.

Credit Suisse would also be subject to enhanced compliance and self-reporting, and the Swiss Financial Market Supervisory Authority (FINMA) would appoint an independent third party to review compliance measures and existing transactions involving weak and corruption-prone countries and companies.

Key takeaways

- Organizations need to have robust AFC policies and procedures in place and ensure their proper execution
- When systemic issues are discovered, cooperation with regulators can lead to a reduction in fines and penalties
- Regulators are cooperating globally to address AFC failures and associated impacts

AML/CFT Cooperation between Countries

FATF Recommendations on Cooperation between Countries

Practices that restrict international cooperation between supervisory authorities or FIUs when analyzing and investigating suspicious transactions and money laundering crimes, confiscating assets, and extraditing accused money launderers are serious obstacles to combating money laundering.

Recommendations 36 through 40 of FATF's 40 Recommendations on establishing and maintaining effective AML/CFT programs pertain specifically to the international aspects of money laundering and terrorist financing investigations. They address mutual legal assistance treaties, extradition, confiscation of assets, and mechanisms to exchange information internationally.

International Money Laundering Information Network

The International Money Laundering Information Network (IMoLIN) serves as a clearinghouse of money laundering information for the benefit of national and international AML agencies. It was developed and is administered by the Global Programme against Money Laundering, Proceeds of Crime, and the Financing of Terrorism of the United Nations Office on Drugs and Crimes on behalf of the UN and other international organizations, including Interpol.

IMoLIN has five main features:

1. **Anti-Money Laundering International Database (AMLID):** A compendium and analysis of national AML laws and regulations, as well as information on national contacts and authorities (the database is password protected)
2. **Reference data:** Research and analysis, bibliography, conventions, legal instruments, and model laws
3. **Country page:** Full text of AML legislation, where available, and links to national FIUs
4. **Calendar of events:** Chronological listing of training events, conferences, seminars, workshops, and other meetings in the AML field
5. **International norms and standards:** Details UN conventions, model laws, and other international standards

Mutual Legal Assistance Treaties

When evidence is required from another jurisdiction, a request can be made for mutual legal assistance. Mutual legal assistance treaties (MLATs) provide a legal basis for transmitting evidence that can be used for prosecution and judicial proceedings. MLATs only involve two countries at a time. For example, the Treaty between Canada and the Kingdom of Spain on Mutual Assistance in Criminal Matters, which has been in force since March 3, 1995, defines criminal matters as "investigations or proceedings relating to offenses concerning taxation, duties, customs and international transfer of capital or payments." Moreover, it defines assistance as the "taking of evidence and obtaining of statements of persons; provision of information, documents and other records, including criminal records, judicial records and government records; location of persons and objects, including their identification; search and seizure; delivery of property, including lending of exhibits; making detained persons and others available to give evidence or assist investigations; service of documents, including documents seeking the attendance of persons; measures to locate, restrain and forfeit the proceeds of crime; and other assistance consistent with the objects of this Treaty."

Procedures can vary, but the typical process for requesting evidence from another jurisdiction involves:

- The central authority of the requesting country sends a *commission rogatoire* (letters rogatory, or letter of request) to the central authority of the other country. The letter includes the information sought, the nature of the request, the criminal charges in the requesting country, and the legal provision under which the request is made.
- The central authority that receives the request sends it to a local financial investigator to determine if the information is available.
- An investigator from the requesting country then visits the country from which the information is sought and accompanies the local investigator during visits or when statements are taken.
- The investigator asks the central authority for permission to remove the evidence to the requesting country.
- The central authority sends the evidence to the requesting central authority, thereby satisfying the request for mutual legal assistance. Local witnesses may need to attend court hearings in the requesting country.

Financial Intelligence Units

FIUs are mandatory national agencies that handle financial intelligence. They receive reports of suspicious transactions from financial organizations, other people, and entities, analyze them, and disseminate the resulting intelligence to local law enforcement agencies and foreign FIUs to combat money laundering.

The first FIUs were established in the early 1990s in response to the need for a central agency to receive, analyze, and disseminate financial information to combat money laundering.

The European FIUs established in the late 90s were predominantly domestically organized and focused. However, to fight the threat posed by criminals and terrorists exploiting the open borders of the EU, the FIUs of Luxembourg, UK, Italy, and France joined the Dutch FIU in its initiative to create a decentralized network for the FIUs to exchange information in a more sophisticated way. With the start of the pilot project in 2004, FIU.net was born.

Starting in 2006, the former Directorate-General Justice, Freedom and Security (DG JLS), later Directorate-General for Migration and Home Affairs (DG HOME) of the European Commission, the Dutch Ministry of Justice and Security, and the participating FIUs funded the EU FIU.net project, which lasted a decade.

During that period the FIU.net Bureau and the project support team, together with the FIUs, developed the FIU.net system into a sophisticated, effective tool in the fight against money laundering and terrorist financing. During those years, they added features to FIU.net, such as Ma3tch, a revolutionary way to match and detect common subjects without exposing information that is not relevant to others. In addition, the Templates feature makes it easy to adjust the system to the specific needs of an individual FIU.

In 2012, FATF adopted a revised set of recommendations on combating money laundering that, for the first time, included explicit recommendations for the establishment and functioning of FIUs. Although the FIU members of the Egmont Group share the same core functions of receiving, analyzing, and disseminating financial information to combat money laundering and financing of terrorism, they often differ in how they are established and how they function. In 2016, the European Union initiated several measures to strengthen the role of FIUs and their ability to share information across Europe as part of its comprehensive action plan toward the fight against terrorism.

Three basic functions of an FIU

FIUs play an important role in the AML/CFT framework. FATF Recommendation 29 states that countries should establish an FIU that serves as a national center for the receipt and analysis of: (a) suspicious transaction reports and (b) other information relevant to money laundering, associated predicate offenses, and terrorist financing, and for the dissemination of the results of that analysis. FIUs should be able to obtain additional information from reporting entities and have access on a timely basis to the financial, administrative, and law enforcement information that it requires to undertake its functions properly.

Articles 30 and 31 of the Recommendations outline the powers of FIUs and other competent authorities responsible for conducting investigations:

- 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 offenses, developing a proactive parallel financial investigation when pursuing money laundering, associated predicate offenses, and terrorist financing, including cases in which the associated predicate offense occurs outside their jurisdictions
- Expeditiously identifying, tracing, and initiating actions to freeze and seize property that is or might become subject to confiscation, or is suspected of being proceeds of crime
- Access to all necessary documents and information for use in those investigations and in prosecutions and related actions, including powers to

use compulsory measures for the production of records held by financial organizations, DNFBPs, and other natural or legal persons for the search of people and premises, taking witness statements, and seizing and obtaining evidence

- Using a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offenses, and terrorist financing, including undercover operations, intercepting communications, accessing computer systems, and controlled delivery.

The Australian Transaction Reports and Analysis Centre (AUSTRAC), founded in 1989, is Australia's primary source for financial intelligence, which is used to fight serious and organized crime and terrorism financing. The UK's FIU is part of the National Crime Agency (NCA). The NCA became operational in 2013 and leads UK law enforcement's fight against serious and organized crime. In the US, FinCEN was established in 1990 with the mission to safeguard the financial system from illicit use, combat money laundering, and promote national security through the collection, analysis, and dissemination of financial intelligence and the strategic use of financial authorities.

FIUs are tasked with receiving and analyzing SARs and maintaining close links with police and customs authorities. They share information among themselves informally in the context of investigations, usually on the basis of memoranda of understanding (MOU). The Egmont Group of FIUs has established a model for MOUs. Unlike the MLATs, MOUs are not typically used for obtaining evidence, but for obtaining intelligence that might lead to evidence.

In June 2001, the members of the Egmont group adopted "Principles of Information Exchange between Financial Intelligence Units" and incorporated the document into its Statement of Purpose. Some countries can restrict the exchange of information with other FIUs or the access to information requested by an FIU. This document describes practices that maximize cooperation among FIUs and can be useful to government authorities when considering AML legislation.

Furthermore, to address practical issues that impede mutual assistance, the document provides best practices for the exchange of information among FIUs. When handling international information requests, FIUs are urged to take these best practices into account.

Key principles included in the document include:

- The Egmont principle of free exchange of information at the FIU level should be possible on the basis of reciprocity, including spontaneous exchange.
- Differences in the definition of offenses that fall under the competence of FIUs should not be an obstacle to the free exchange of information at the FIU level. To this end, the FIU's competence should extend to all predicate offenses for money laundering, as well as terrorist financing.
- The exchange of information among FIUs should take place as informally and as rapidly as possible and with no excessive formal prerequisites, while guaranteeing protection of privacy and confidentiality of the shared data.
- When an FIU needs a memorandum of understanding to exchange information, it should be negotiated and signed by the FIU without undue delay. To that end, the FIU should have the authority to sign MOUs independently.
- It should be possible for communication among FIUs to take place directly, without intermediaries.
- Providing an FIU's consent to disseminate the information for law enforcement or judicial purposes should be granted promptly and to the greatest extent possible. The FIU providing the information should not deny permission to disseminate the information unless doing so would fall beyond the scope of its AML/CFT provisions; could impair a criminal investigation; would be clearly disproportionate to the legitimate interests of an individual, legal person, or the country of the providing FIU; or would otherwise not be in accord with basic principles of national law. Any refusal to grant consent should be appropriately explained.

The following practices should be observed by the FIU requesting the information:

- All FIUs should submit requests for information in compliance with the Principles of Information Exchange established by the Egmont Group.

When applicable, the provisions of information-sharing arrangements among FIUs should also be observed.

- Requests for information should be submitted as soon as the precise assistance required is identified.
- When an FIU has information that might be useful to another FIU, it should consider supplying it spontaneously as soon as the relevance of sharing this information is identified.
- The exchange of information among Egmont FIUs should take place in a secure way. To this end, the Egmont FIUs should use the Egmont Secure Web (ESW) when appropriate.

The Egmont Group released a revised charter that built on the original one and included updates to:

- Unite efforts to improve an effective exchange of information upon request and spontaneously to combat money laundering and financing of terrorism.
- Exchange information on their respective experiences to promote the development of effective FIUs.
- Support the Egmont Group members to enhance their capacity by promoting operational independence of FIUs, offering training and technical assistance, promoting personnel exchanges, developing operational and strategic collaboration, and maintaining and granting access to a secure channel for information exchange among Egmont Group FIUs.

An example of FIUs collaborating and utilizing MOUs was in October 2013, when FinCEN and Mexico's National Banking and Securities Commission executed the first-ever MOU to facilitate the exchange of supervisory information in support of both agencies' AML/CFT missions. Moreover, it provided for strict controls and safeguards to ensure that shared information is well protected and used in a confidential and authorized manner for AML/CFT supervision purposes only.

Appendix

Additional Study Resources

This section cites several CAMS Examination supporting documents and reference materials. It also suggests websites and periodicals that offer additional supporting material. Several international bodies that are focused on AML/CFT have published valuable guidance documents and reference materials that are helpful in preparing for the CAMS Examination.

For study purposes, generally the reference documents have an introduction, putting the material in context and, in some cases, describing the methodology behind their production. For example, in each of FATF's Risk-Based Approach Guidance documents, the purpose of the risk-based approach is explained in the opening chapter. The core material then describes the specific AML risks that are the focus of the guidance and describes the best practices for mitigating those risks. It is this core material that is examined in the CAMS Examination.

Two documents above all others (FATF's 40 Recommendations and Interpretive Notes) should receive particular study from CAMS candidates. It is highly advised to download the free .pdf versions available from the FATF website to keep with your other CAMS study materials. The 40 Recommendations are the basic elements of every AML regime at the national and financial institution levels and most of the other materials build off specific aspects of this foundation.

Guidance documents and reference materials

- United Nations:
  - Model legislation on money laundering and financing of terrorism
  - UN Security Council Resolutions on Terrorism
  - United Nations Convention against Corruption (2003)
  - United Nations Convention against Transnational Organized Crime (Palermo Agreement) (2000)
- European Union:
  - Fifth EU Money Laundering Directive: Directive (EU) 2018/843
  - Fourth EU Money Laundering Directive: Directive (EU) 2015/849
  - Cash Control Regulation: (EU) 2018/1672
  - Regulation on information on the payer accompanying transfers of funds: (EU) 2015/847
  - Third EU Directive 2005/60/EC of the European Parliament and of the Council
  - Joint Action (1998) on money laundering and the identification, tracing, freezing, seizing, and confiscation of instrumentalities and the proceeds from crime, and its subsequent amendment
  - Regulation (2001) on restrictive measures for combating terrorism, and its amending Regulation 2003
  - Framework Decision (2000) on cooperation among European FIUs
- United States:
  - The Anti-Money Laundering Act of 2020 (AMLA)
  - USA PATRIOT Act 2001
  - Bank Secrecy Act 1970
  - FinCEN
    - CDD Final Rule and FAQs

        - Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies 2019
        - Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern
        - Advisories, notices, bulletins, and fact sheets
        - Frequently asked questions (FAQs)
    - US Department of the Treasury
        - Terrorism and money laundering risk assessments
        - Money laundering threat assessment
        - Best practices
        - Industry specific guidance on the risk-based approach
    - FINRA
        - Notices and guidance
        - Frequently asked questions (FAQs)
- United Kingdom:
    - The Money Laundering and Terrorist Financing (Amendment) Regulations 2019
    - JMSLG: The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
    - The Terrorism Act 2000 and Proceeds of Crime Act 2002
    - Proceeds of Crime Act 2002
- Basel Committee
    - Sound Management of Risks Related to Money Laundering and Financing of Terrorism: Revisions to Supervisory Cooperation, 2020
    - Sound Management of Risks Related to Money Laundering and Financing of Terrorism: Revisions to Correspondent banking Annex, 2017
    - General Guide to Account Opening, 2016
    - Sound Management of Risks Related to Money Laundering and Financing of Terrorism, 2016

- Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers, 2009
- Compliance and the Compliance Function in Banks, 2005
- Initiatives by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism, 2005
- Consolidated KYC Risk Management, 2004
- General Guide to Account Opening and Customer Identification, 2003
- Sharing of Financial Records between Jurisdictions in Connection with the Fight against Terrorist Financing, 2002
- Customer Due Diligence for Banks, 2001

- Egmont Group
  - FIU's in Action: 100 Cases from the Egmont Group
  - ECOFEL: Financial Investigations into Wildlife Crime, 2021
  - Customs: FIU Cooperation Handbook, 2020
  - Public Bulletin: Combatting Online Child Sexual Abuse and Exploitation through Financial Intelligence, 2020
  - Public Bulletin: Money Laundering of Serious Tax Crimes, 2020
  - Egmont Group Bulletin: Professional Money Laundering Facilitators, 2019
- Financial Action Task Force (FATF):
  - Mutual Evaluation Reports
  - High-Risk and Other Monitored Jurisdictions
  - The Forty Recommendations and Interpretative Notes
  - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, 2020
  - Money Laundering and the Illegal Wildlife Trade, 2020
  - FATF/Egmont Trade-based Money Laundering: Trends and Developments, 2020
  - The FATF Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, 2019

- Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2019
- Best Practices on Beneficial Ownership for Legal Persons, 2019
- Money Laundering and Terrorist Financing Risks, 2019
- Terrorist Financing Risk Assessment Guidance, 2019
- Financial Flows from Human Trafficking, 2018
- Guidance for a Risk-Based Approach: Life Insurance Sector, 2018
- Risk of Terrorist Abuse in Non-Profit Organisations, 2014
- Virtual Currencies: Key Definitions and Potential AML/CFT Risks, 2014

- Wolfsberg Group:
  - Wolfsberg correspondent banking due diligence questionnaire (Wolfsberg CBDDQ)
  - Guidance on Customer Tax Evasion, 2019
  - ICC and BAFT Trade Finance Principles, 2019
  - Guidance on Politically Exposed Persons (PEPs), 2017
  - Anti-bribery and Corruption (ABC) Compliance Programme Guidance, 2017
  - Anti-Money Laundering Principles for Correspondent Banking, 2014
  - Guidance on Mobile and Internet Payment Services (MIPS), 2014
  - Anti-Money Laundering Principles for Private Banking, 2012
  - Statement on the Suppression of the Financing of Terrorism, 2002
- FATF-style regional bodies typology reports

Other websites with helpful AML material

CAMS qualified professionals will routinely consult the websites of their home regulators. However, there are other websites that contain helpful AML materials. Just *copy and paste the title into your browser window* to find the most recent URL.

- ACAMS
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
- International Monetary Fund
- UK Financial Conduct Authority
- U.S. Financial Crimes Enforcement Network home page
- U.S. Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering InfoBase
- U.S. Office of Foreign Assets Control (OFAC)
- World Bank

AML-related periodicals

- *ACAMS Today*

  A quarterly magazine for ACAMS members providing stories from the AML workplace and current global issues and developments on money laundering.

- ACAMS MoneyLaundering.com

  A monthly newsletter focusing on current global, legal, regulatory and enforcement issues and other money laundering-related news, analysis and guidance.

- *Money Laundering Bulletin*

  A UK-based newsletter published 10 times per year addressing issues on money laundering practices, policing efforts and the anti-laundering systems of various industries.

- *ABA Bank Compliance*

  The American Bankers Association's monthly magazine dealing with legal, regulatory and compliance issues and information.

Glossary

Affidavit

A written statement given under oath before an officer of the court, notary public or other authorized person. It is commonly used as the factual basis for an application for a search, arrest or seizure warrant.

Alternative remittance system (ARS)

Underground banking or informal value transfer systems (IVTS). Often associated with ethnic groups from the Middle East, Africa or Asia, and commonly involves the transfer of values among countries outside of the formal banking system. The remittance entity can be an ordinary shop selling goods that has an arrangement with a correspondent business in another country. There is usually no physical movement of currency and a lack of formality with regard to verification and record keeping. The money transfer takes place by coded information that is passed through chits, couriers, letters, faxes, emails, text messages or online chat systems, followed by some form of telecommunications confirmations.

Anti-money laundering and counter-financing of terrorism program

See anti-money laundering program

Anti-Money Laundering International Database (AMLID)

A compendium of analyses of anti-money laundering laws and regulations, including two general classes of money laundering control measures—domestic laws and international cooperation—as well as information on national contacts and authorities. A secure, multilingual database, AMLID is an important reference tool for law enforcement officers involved in cross-jurisdictional work.

Anti-money laundering program

The system designed to assist institutions in their fight against money laundering and terrorist financing. In many jurisdictions, government regulations require financial institutions, including banks, securities dealers and money services businesses, to establish such programs. At a minimum, the anti-money laundering program should include:

1. written internal policies, procedures and controls;
2. a designated AML compliance officer;
3. ongoing employee training and
4. independent review to test the program

Arrest warrant

A court order directing a law enforcement officer to seize and detain a particular person and require him or her to provide an answer to a complaint or otherwise appear in court.

Asia/Pacific Group on Money Laundering (APG)

A Financial Action Task Force (FATF)-style regional body consisting of jurisdictions in the Asia/Pacific Region.

Asset protection

A process that includes reorganizing how assets are held in order to make them less vulnerable should a claim be made against a person. Asset protection is also a term used by tax planners for measures taken to protect assets from taxation in other jurisdictions.

Asset protection trusts (APTs)

A special form of irrevocable trust usually created (i.e., settled) offshore for the principal purposes of preserving and protecting part of one's wealth from creditors. Title to the asset is transferred to a person named the trustee. APTs are generally used for asset protection and are usually tax neutral. Their ultimate function is to provide for the beneficiaries. Some proponents advertise APTs as allowing foreign trustees to ignore U.S. court orders and to simply transfer the trust to another jurisdiction in response to legal action threatening the trust's assets.

Automated Clearing House (ACH)

An electronic banking network that processes large volumes of both credit and debit transactions that originate in batches. ACH credit transfers include direct deposit payroll payments and payments to contractors and vendors. ACH debit transfers include consumer payments on insurance premiums, mortgage loans and other kinds of expenses.

Automated teller machine (ATM)

An electronic banking outlet that allows customers to complete basic transactions without the assistance of a bank employee. ATMs generally dispense cash, allow check and cash deposits and transfers to be made, as well as balance inquiries.

Bank draft

Vulnerable to money laundering because it represents a reputable international monetary instrument drawn on a reputable institution, and is often made payable—in cash—upon presentation and at the issuing institution's account in another country.

Bank secrecy

Refers to laws and regulations in countries that prohibit banks from disclosing information about an account—or even revealing its existence—without the consent of the account holder. Impedes the flow of information across national borders among financial institutions and their supervisors. One of FATF's 40 Recommendations states that countries should ensure that secrecy laws do not inhibit the implementation of the FATF Recommendations.

Bank Secrecy Act (BSA)

The primary U.S. anti-money laundering regulatory statute (Title 31, U.S. Code Sections 53115355) enacted in 1970 and most notably amended by the USA PATRIOT Act in 2001. Among other measures, it imposes money laundering controls on financial institutions and many other businesses, including the requirement to report and to keep records of various financial transactions.

Bank Secrecy Act (BSA) compliance program

A program that U.S.-based financial institutions—as defined by the Bank Secrecy Act—are required to establish and implement in order to control money laundering and related financial crimes. The program's components include at a minimum: the development of internal policies, procedures and controls; the designation of a compliance officer; ongoing employee training and an independent audit function to test the program.

Basel Committee on Banking Supervision (Basel Committee)

The Basel Committee was established by the G-10's central bank of governors in 1974 to promote sound supervisory standards worldwide. Its Secretariat is appointed by the Bank for International Settlements in Basel, Switzerland. It has issued, among others, papers on customer due diligence for banks, consolidated KYC risk management, transparency in payment messages, due diligence and transparency regarding cover payment messages related to cross-border wire transfers and sharing of financial records among jurisdictions in connection with the fight against terrorist financing. See www.bis.org/bcbs.

Batch processing

A type of data processing and data communications transmission in which related transactions are grouped together and transmitted for processing, usually by the same computer and under the same application.

Bearer form

In relation to a certificate, share transfer or other document, a bearer form enables a designated investment or deposit to be sold, transferred, surrendered or addressed to a bearer without the need to obtain further written instructions.

Bearer negotiable instruments

Includes monetary instruments in bearer form such as: negotiable instruments (including checks, promissory notes and money orders) that are either in bearer form, are endorsed without restriction, are made out to a payee or are otherwise in such form that title thereto passes upon delivery.

Bearer share

Negotiable instruments that accord ownership in a corporation to the person who is in physical possession of the bearer share certificate, a certificate made out to Bearer and not in the name of an individual or organization.

Benami account

Also called a nominee account. Held by one person or entity on behalf of another or others, Benami accounts are associated with the hawala underground banking system of the Indian subcontinent. A person in one jurisdiction seeking to move funds through a hawaladar to another jurisdiction may use a Benami account or Benami transaction to disguise his or her true identity or the identity of the recipient of the funds.

Beneficial owner

The term beneficial owner has two different definitions depending on the context.

- The natural person who ultimately owns or controls an account through which a transaction is being conducted.
- The natural people who have significant ownership of, as well as those who exercise ultimate effective control over, a legal person or arrangement.

Beneficiary

The term beneficiary has two different definitions depending on the context.

- The person (natural or legal) who benefits from a transaction, such as the party receiving the proceeds of a wire, a payout on an insurance policy.
- In the trust context, all trusts (other than charitable or statutory-permitted noncharitable trusts) must have beneficiaries, which may include the settlor. Trusts must also include a maximum time frame, known as the perpetuity period, which normally extends up to 100 years. Although trusts

must always have some ultimately ascertainable beneficiary, they may have no defined existing beneficiaries.

Bill stuffing

A casino customer goes to various slot machines putting cash in the bill acceptors and collects cash-out tickets with nominal gaming activity, then cashes out at the casino cage or asks for a check.

Black Market Peso Exchange (BMPE)

The Black Market Peso Exchange (BMPE) is an example of a complex method of trade-based money laundering. The BMPE originally was driven by Colombia's restrictive policies on currency exchange. To circumvent those policies, Colombian businesses bypassed the government levies by dealing with peso brokers that dealt in the black market or parallel financial market. Colombian drug traffickers took advantage of this method to receive Colombian pesos in Colombia in exchange for U.S. drug dollars located in the U.S.

Cardholder

Person to whom a financial transaction card is issued, or an additional person authorized to use the card.

Caribbean Financial Action Task Force (CFATF)

An FATF-style regional body comprising Caribbean nations, including Aruba, the Bahamas, the British Virgin Islands, the Cayman Islands and Jamaica.

Casa de cambio

Also called a bureau de change or an exchange office, a casa de cambio offers a range of services that are attractive to money launderers: currency exchange and consolidation of small denomination bank notes into larger ones; exchange of financial instruments such as travelers checks, money orders and personal checks; and telegraphic transfer facilities.

Cash collateralized loans

A cash collateralized loan has cash deposits as the loan's collateral. The cash deposits can sometimes reside in another jurisdiction.

Cash deposits

Sums of currency deposited in one or more accounts at a financial institution. Vulnerable to money laundering in the placement phase, as criminals move their cash into the noncash economy by making deposits into accounts at financial institutions.

Cashier's check

Common monetary instrument often purchased with cash. Can be used for laundering purposes, cashier's checks provide an instrument drawn on a financial institution.

Cash-intensive business

Any business in which customers usually pay with cash for the products or services provided, such as restaurants, pizza delivery services, taxi firms, coin-operated machines or car washes. Some money launderers run or use cash-based businesses to commingle illegally obtained funds with cash actually generated by the business.

CICAD (Comisión Interamericana para el Control del Abuso de Drogas or Inter-American Drug Abuse Control Commission)

CICAD has issued several sets of anti-money laundering recommendations, including amendments to the Organization of American States (OAS) Model Regulations issued in 1992.

Collection accounts

Immigrants from foreign countries deposit many small amounts of currency into one account where they reside, and the collected sum is transferred to an account in their home country without documentation of the sources of the funds. Certain ethnic groups from Asia or Africa may use collection accounts to launder money.

Commission rogatoire

Also known as letters rogatory, a commission rogatoire is a written request for legal or judicial assistance sent by the central authority of one country to the central authority of another when seeking evidence from the foreign jurisdiction. The letter typically specifies the nature of the request, the relevant criminal charges in the requesting country, the legal provision under which the request is made, and the information sought.

Concentration account

Also called an omnibus account. Held by a financial institution in its name, a concentration account is used primarily for internal administrative or bank-to-bank transactions in which funds are transmitted and commingled without personally identifying the originators.

Concentration risk

Concentration risk primarily applies to the asset side of the balance sheet. As a common practice, supervisory authorities not only require financial institutions to have information systems to identify credit concentrations, but also set limits to restrict bank exposure to single borrowers or groups of related borrowers. On the liability side, concentration risk is associated with funding risk, especially the risk of early and sudden withdrawal of funds by large depositors that could harm an institution's liquidity.

Confidentiality

Keeping certain facts, data and information out of public or unauthorized view. In most jurisdictions, confidentiality is required when filing suspicious transaction or activity reports –the filing institution's employees cannot notify a customer that a report has been filed. In another context, a breach of confidentiality can occur when an institution discloses client information to enforcement agencies or a financial intelligence unit in violation of the jurisdiction's bank secrecy laws.

Confiscation

Includes forfeiture where applicable, and means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to the state. Upon transfer, the individual(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture lose all rights, in principle, to the confiscated or forfeited assets.

Corporate vehicles

Types of legal entities that may be subject to misuse such as private limited companies and public limited companies whose shares are not traded on a stock exchange, trusts, nonprofit organizations, limited partnerships and limited liability partnerships and private investment companies. Occasionally, it is difficult to identify the people who are the ultimate beneficial owners and controllers of corporate vehicles, which makes the vehicles vulnerable to money laundering.

Correspondent banking

The provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Large international banks typically act as correspondents for hundreds of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers of funds, check clearing services, payable-through accounts and foreign exchange services.

Credit cards

A plastic card with a credit limit used to purchase goods and services and to obtain cash advances on credit. The cardholder is subsequently billed by the issuer for repayment of the credit extended. Credit cards may be used to launder money when payments of the amounts owed on the card are made with criminal money.

Criminal proceeds

Any property derived from or obtained, directly or indirectly, through the commission of a crime.

Cross border

Used in the context of activities that involve at least two countries, such as wiring money from one country to another or taking currency across a border.

Currency

Banknotes and coins that are in circulation as a medium of exchange.

Currency smuggling

The illicit movement of large quantities of cash across borders, often into countries without strict banking secrecy, poor exchange controls or poor anti-money laundering legislation.

Currency transaction report (CTR)

A report that documents a physical currency transaction that exceeds a certain monetary threshold. A CTR can also be filed on multiple currency transactions that occur in one day exceeding the required reporting amount. Some countries, including the U.S., have requirements addressing when CTRs should be filed with government authorities.

Custodian

A bank, financial institution or other entity that is responsible for managing, administering or safekeeping assets for other people or institutions. A custodian holds assets to minimize risk of theft or loss, and does not actively trade or handle the assets.

Custody

The act of or authority to safeguard and administer clients' investments or assets.

Customer due diligence (CDD)

In terms of money laundering controls, CDD requires policies, practices and procedures that enable a financial institution to predict with relative certainty the types of transactions in which the customer is likely to engage. CDD includes not only establishing the identity of customers, but also establishing a baseline of account activity to identify those transactions that do not conform to normal or expected transactions.

Debit card

A card that permits an account holder to draw funds from an existing account. Debit cards are used to pay obligations or make purchases. Debit cards can be used in a variety of places, including on the Internet. Debit cards often allow for movement of cash via cash-back transactions or withdrawals at ATMs.

Designated Categories of Offense

Those crimes considered by FATF to be money-laundering predicate offenses. Each country can separately decide how it will define specific offenses and their elements under its own domestic laws. Many nations do not specify which crimes can serve as predicates for laundering prosecutions and merely state that all serious felonies may be predicates.

Designated nonfinancial businesses and professions

FATF recommends certain standards apply to nonfinancial businesses and professions, including specifically:

- casinos (including Internet casinos);
- real estate agents;
- dealers in precious metals and precious stones;
- lawyers, notaries, other independent legal professionals and accountants (Refers to those who prepare or carry out certain duties on behalf of clients); and
- trust and company service providers who prepare or carry out certain duties on behalf of their clients.

Domestic transfer

Electronic funds transfer in which the originator and beneficiary institutions are located in the same jurisdiction. A domestic transfer therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the actual system used to send the wire transfer may be located in another jurisdiction or online.

Eastern and Southern African Anti-Money Laundering Group (ESAAMLG)

An FATF-style regional body comprising countries from the Eastern region of Africa down to the Southern tip of Africa, established in 1999.

Egmont Group of Financial Intelligence Units

The Egmont Group consists of numerous national financial intelligence units (FIUs) that meet regularly to find ways to promote the development of FIUs and to cooperate, especially in the area of information exchange, training and the sharing of expertise. The goal of the group is to provide a forum for FIUs to improve cooperation in the fight against money laundering and the financing of terrorism, and to foster the implementation of domestic programs in this field.

Electronic funds transfer (EFT)

The movement of funds between financial institutions electronically. The two most common electronic funds transfer systems in the U.S. are FedWire and CHIPS. (SWIFT is often referred to as the third EFT system, but in reality it is an international messaging system that carries instructions for wire transfers between institutions, rather than the wire transfer system itself.)

Electronic money (emoney)

Electronic cash represents a series of monetary value units in some electronic format, such as being stored electronically online, on the hard drive of a device or on the microchip of a plastic card.

Enhanced due diligence (EDD)

In conjunction with customer due diligence, EDD calls for additional measures aimed at identifying and mitigating the risk posed by higher risk customers. It requires developing a more thorough knowledge of the nature of the customer, the customer's business and understanding of the transactions in the account than a standard or lower risk customer. A financial institution should ensure account profiles are current and monitoring should be risk-based.

Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)

An FATF-style regional body formed in October 2004 in Moscow.

European Union (EU)

The modern EU was founded in the Treaty of Maastricht on European Union, signed in 1992 and effective in 1993. The EU is a politico-economic union of member states located primarily in Europe. Member states have set up three common institutions (the European Parliament, the European Commission and the Council of the European Union) to which they delegate part of their sovereignty so that decisions on specific matters of collective interest can be made democratically at the European level. As a result, people, goods, services and money flow freely through the EU.

European Union Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing

First adopted by the European Union in June 1991 and updated in 1997, 2005 and 2015, the Directive requires EU member states to ensure that money laundering and terrorist financing are prohibited. The Directive applies to a broad spectrum of entities, including financial institutions, accountants, notaries, trust companies, estate agents and some providers of gambling services. Member states are expected to identify and mitigate risks appropriately. They are to oversee financial institutions and other obliged entities, including establishing standards for customer due diligence, prohibition of shell banking relationships, establishing FIUs, developing standards for document retention and requiring consequences for failure to comply.

Europol

Europol is the EU's law enforcement agency. Its main goal is to help achieve a safer Europe for the benefit of all EU citizens. In the area of anti-money laundering, Europol provides member states' law enforcement authorities with operational and analytical support via the Europol liaison officers (ELOs) and its analysts, as well as state-of-the-art databases and communication channels.

Express trust

A trust created expressly by the settlor, usually in the form of a document such as a written deed of trust. An express trust differs from trusts that do not result from the specific intent or decision of a settlor to create a trust (e.g., constructive trust established by a court of law to address undeclared property).

Extradition

The surrender by one jurisdiction to another of an accused or convicted person under an agreement that specifies the terms of such exchanges.

Extraterritorial reach

The extension of one country's policies and laws to the citizens and institutions of another. Depending on jurisdiction, money laundering laws may extend prohibitions and sanctions into other jurisdictions.

Financial Action Task Force (FATF)

FATF was chartered in 1989 by the Group of Seven industrial nations to foster the establishment of national and global measures to combat money laundering. It is an international policy making body that sets anti-money laundering standards and counter-terrorist financing measures worldwide. Its Recommendations do not have the force of law. Thirty-five countries and two international organizations are members. In 2012, FATF substantially revised its 40 + 9 Recommendations and reduced them to 40. FATF develops annual typology reports showcasing current money laundering and terrorist financing trends and methods. *See www.fatf-gafi.org.*

Financial Action Task Force on Money Laundering in Latin America (GAFILAT)

An FATF-style regional body for Latin America, established in 2000.

Financial Action Task Force-Style Regional Body (FSRB)

FSRBs have forms and functions similar to those of FATF. However, their efforts are targeted to specific regions. In conjunction with FATF, FSRBs constitute an affiliated global network to combat money laundering and terrorist financing.

Financial intelligence unit (FIU)

A central national agency responsible for receiving, analyzing and transmitting disclosures on suspicious transactions to appropriate authorities.

Forfeiture

The involuntary loss of property or assets as a result of legal action. Generally, the owner of the property that has failed to comply with the law or the property is linked to some sort of criminal activity.

Freeze

To prevent or restrict the exchange, withdrawal, liquidation or use of assets or bank accounts. Unlike forfeiture, frozen property, equipment, funds or other assets remain the property of the natural or legal people that held an interest in them at the time of the freezing and may continue to be administered by third parties. The courts may decide to implement a freeze as a means to protect against flight.

Front company

Any business set up and controlled by another organization. Although not necessarily illicit, criminals use front companies to launder money by giving the funds the appearance of legitimate origin. Front companies may subsidize products and services at levels well below market rates or even below manufacturing costs.

GAFISUD (Spanish: Grupo de Acción Financiera de Sudamérica)

See Financial Action Task Force on Money Laundering in Latin America.

Gatekeepers

Professionals, such as lawyers, notaries, accountants, investment advisors and trust and company service providers, who assist in transactions involving the movement of money and are deemed to have a particular role in identifying, preventing and reporting money laundering. Some countries impose due diligence requirements on gatekeepers that are similar to those of financial institutions.

Grantor

The party who transfers title or ownership of property or assets. In a trust, typically the person who creates or funds the trust.

Gulf Cooperation Council (GCC)

Formed in 1981, the GCC promotes cooperation between its member states in the fields of economy and industry. Member states include Kuwait, Bahrain, Qatar, Saudi Arabia, Oman and the United Arab Emirates. The GCC is a member of FATF, although its individual members are not.

Hawala

An informal value transfer system common in the Middle East, North Africa and the Indian subcontinent. The system operates outside traditional banking systems. In a basic form, a customer contacts a hawaladar and gives him or her money to be transferred to another person. The hawaladar contacts his or her counterpart where the second person lives, who remits the funds to that person. A running tally is kept between the hawaladars of which owes the other a net sum. *See alternative remittance system.*

Hawaladar

A hawala broker.

Human smuggling

Human smuggling refers to the transport or illegal entry of a person across international borders in contravention of one or more countries' laws. Human smuggling differs from human trafficking in that it focuses on the entry or transport, rather than the exploitation, of the person involved.

Human trafficking

Also known as Trafficking in Persons. The trade of humans, most commonly for the purpose of sexual slavery, forced labor or commercial sexual exploitation. Trafficking occurs in almost every country in the world and is often cited as the second-largest criminal enterprise in the world.

Informal value transfer system (IVTS)

See alternative remittance system.

Integration

The integration phase, often referred to as the third and last stage of the classic money laundering process, places laundered funds back into the economy by re-entering the funds into the financial system and giving them the appearance of legitimacy.

International business company (IBC)

A variety of offshore corporate structures that are dedicated to business use outside the incorporating jurisdiction and feature rapid formation, secrecy, broad powers, low cost, low-to-zero taxation and minimal filing and reporting requirements.

International Monetary Fund (IMF)

An organization of more than 180 member countries, the IMF works to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth and reduce poverty around the world. The organization's objectives have remained unchanged since it was established. Its operations, which involve surveillance, financial assistance and technical support, have adjusted to meet the changing needs of member countries.

Know your customer (KYC)

Anti-money laundering policies and procedures used to determine the true identity of a customer and the type of activity that is normal and expected, and to detect activity that is unusual for a particular customer.

Know your employee (KYE)

Anti-money laundering policies and procedures for acquiring a better knowledge and understanding of the employees of an institution for the purpose of detecting conflicts of interests, money laundering, past criminal activity and suspicious activity.

Knowledge

Mental state accompanying a prohibited act. The Interpretive Notes to Recommendation 3 of the FATF 40 Recommendations of 2012 say that countries should ensure that the intent and knowledge required to prove the offense of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such a mental state may be inferred from objective factual circumstances. The exact definition of knowledge that accompanies an anti-money laundering act varies by country. Knowledge can be deemed, under certain circumstances, to include willful blindness; that is "the deliberate avoidance of knowledge of the facts," as some courts have defined the term.

Layering

The second phase of the classic three-step money laundering process between placement and integration, layering involves distancing illegal proceeds from their source by creating complex levels of financial transactions designed to disguise the audit trail and to provide anonymity.

Legal risk

Defined by the 2001 Basel Customer Due Diligence for Banks paper as the possibility that lawsuits, adverse judgments or contracts that cannot be enforced may disrupt or harm a financial institution. In addition, banks can suffer administrative or criminal penalties imposed by the government. A court case involving a bank may have graver implications for the institution than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not practice due diligence in identifying customers and understanding and managing their exposure to money laundering.

Letter of credit

A credit instrument issued by a bank that guarantees payments on behalf of its customer to a third party when certain conditions are met.

Letter rogatory

See commission rogatoire.

Memorandum of understanding (MOU)

Agreement between two parties establishing a set of principles that govern their relationship on a particular matter. An MOU is often used by countries to govern their sharing of assets in international asset-forfeiture cases or to set out their respective duties in anti-money laundering initiatives. Financial intelligence units (FIUs), with the task of receiving and analyzing suspicious transaction reports on an ongoing basis and maintaining close links with police and customs authorities, share information among themselves informally in the context of investigations, usually on the basis of an MOU.

Middle East and North Africa Financial Action Task Force (MENAFATF)

A FATF-style body established for the Middle Eastern and North African regions in 2004.

Monetary instruments

Traveler's checks, negotiable instruments, including personal checks and business checks, official bank checks, cashier's checks, promissory notes, money orders, securities or stocks in bearer form. Monetary instruments are normally included, along with currency, in the antimoney laundering regulations of most countries, and financial institutions must file reports and maintain records of customer activities involving them.

Money laundering

The process of concealing or disguising the existence, source, movement, destination or illegal application of illicitly derived property or funds to make them appear legitimate. It usually involves a three-part system: placement of funds into a financial system, layering of transactions to disguise the source, ownership and location of the funds and integration of the funds into society in the form of holdings that appear legitimate. The definition of money laundering varies in each country where it is recognized as a crime.

Money laundering reporting officer (MLRO)

A term used in various international rules to refer to the person responsible for overseeing a firm's anti-money laundering activities and program and for filing reports of suspicious transactions with the national FIU. The MLRO is the key person in the implementation of anti-money laundering strategies and policies.

Money order

A monetary instrument usually purchased with cash in small (generally under 500 euros) denominations. It is commonly used by people without checking accounts to pay bills or to pay for purchases in which the vendor will not accept a personal check. Money orders may be used for laundering because they represent an instrument drawn on the issuing institution rather than on an individual's account.

Money services business (MSB)

A person (whether a natural or legal person) engaged in any of the following activities where it exceeds the applicable regulatory threshold, at which point the person is generally deemed to be a financial institution subject to AML obligations.

- Dealing in foreign exchange
- Check cashing
- Issuing or selling traveler's checks or money orders
- Providing or selling prepaid access
- Money transmission

Money transfer service or value transfer service

Financial service that accepts cash, checks and other monetary instruments that can store value in one location and pay a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third-party final payment. A money or value transfer service may be provided by people (natural or legal) formally through the regulated financial system (e.g., bank accounts), informally through nonbank financial institutions and business entities or outside of the regulated system. In some jurisdictions, informal systems are referred to as alternative remittance services or underground (or parallel) banking systems.

MONEYVAL

Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures. Formerly PC-R-EV, the committee was established in 1997 by the Committee of Ministers of the Council of Europe to conduct self and mutual assessments of anti-money laundering measures in place in Council of Europe countries that are not FATF members. MONEYVAL is a sub-committee of the European Committee on Crime Problems of the Council of Europe (CDPC).

Monitoring

An element of an institution's anti-money laundering program in which customer activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are often monitored using software that weighs the activity against a threshold of what is deemed normal and expected for the customer.

Mutual legal assistance treaty (MLAT)

Agreement among countries allowing for mutual assistance in legal proceedings and access to documents and witnesses and other legal and judicial resources in the respective countries, in private and public sectors, for use in official investigations and prosecutions.

Nesting

The practice where a respondent bank provides downstream correspondent services to other financial institutions and processes these transactions through its own correspondent account. The correspondent bank is thus processing transactions for financial institutions on which it has not conducted due diligence. Although this is a normal part of correspondent banking, it requires the correspondent bank to conduct enhanced due diligence on its respondent's AML program to adequately mitigate the risk of processing the customer's customers' transactions.

Nongovernmental organization (NGO)

Nonprofit organizations that are not directly linked to the governments of specific countries, and perform a variety of service and humanitarian functions, including bringing citizen concerns to governments, advocating for causes and encouraging political participation. Some countries' antimoney laundering regulations for NGOs still have loopholes that some worry could be exploited by terrorists or terrorist sympathizers trying to secretly move money.

Nonprofit organizations (NPO)

These can take on a variety of forms, depending on the jurisdiction and legal system, including associations, foundations, fund-raising committees, community service organizations, corporations of public interest, limited companies and public benevolent institutions. FATF has suggested practices to help authorities protect organizations that raise or disburse funds for charitable, religious, cultural, educational, social or fraternal purposes from being misused or exploited by financiers of terrorism.

Offshore

Literally, away from one's own home country—if one lives in Europe, the United States is offshore. In the money laundering lexicon, the term refers to jurisdictions deemed favorable to foreign investments because of low or no taxation or strict bank secrecy regulations.

Offshore banking license

A license that prohibits a bank from doing business with local citizens or in local currency as a condition of its license.

Offshore financial center (OFC)

Institutions that cater to or otherwise encourage banks, trading companies and other corporate or legal entities to physically or legally exist in a jurisdiction but limit their operations to offshore, meaning outside the jurisdiction (*see offshore*). OFCs have historically been located in the Caribbean or on Mediterranean islands to be in reasonable proximity to the major financial centers of the U.S. and Europe.

Omnibus account

See clearing account.

Operational risk

The risk of direct or indirect loss of operations due to inadequate or failed internal processes, people or systems, or as a result of external events. Public perception that a bank is not able to manage its operational risk effectively can disrupt or harm the business of the bank.

Organization for Economic Cooperation and Development (OECD)

International organization that assists governments on economic development issues in the global economy. OECD houses the FATF Secretariat in Paris.

Originator

The account holder or, where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

Payable through account

Transaction account opened at a depository institution by a foreign financial institution through which the foreign institution's customers engage, either directly or through subaccounts, in banking activities and transactions in such a manner that the financial institution's customers have direct control over the funds in the account. These accounts pose risks to the depository institutions that hold them because it can be difficult to conduct due diligence on foreign institution customers who are ultimately using the PTA accounts.

Physical presence

Existence of an actual brick-and-mortar location with meaningful management of the institution physically located within a country, where it maintains business records and is subject to supervision. The mere existence of a local agent or low level staff does not constitute physical presence.

Placement

The first phase of the money laundering process: The physical disposal of proceeds derived from illegal activity.

Politically exposed person (PEP)

According to FATF's revised 40 Recommendations of 2012, a PEP is an individual who has been entrusted with prominent public functions in a foreign country, such as a head of state, senior politician, senior government official, judicial or military official, senior executive of a state-owned corporation or important political party official, as well as their families and close associates. The term PEP does not extend to middle-ranking individuals in the specified categories. Various country regulations will define the term PEP, which may include domestic as well as foreign persons.

Ponzi scheme

A money laundering system named after Charles Ponzi, an Italian immigrant who spent 10 years in jail in the U.S. for a scheme that defrauded 40,000 people out of $15 million. Ponzi's name became synonymous with the use of new investors' money to pay off prior investors. Ponzi schemes involve fake, nonexistent investment schemes in which the investors are tricked into investing on the promise of unusually attractive returns. The operator of the scheme can keep the operation going by paying off early investors with the money from new investors until the scheme collapses under its own weight and/or the promoter vanishes with the remaining money.

Predicate crimes

Specified unlawful activities whose proceeds, if involved in the subject transaction, can give rise to prosecution for money laundering. Most anti-money laundering laws contain a wide definition or listing of such underlying crimes. Predicate crimes are sometimes defined as felonies or "all offenses in the criminal code."

Private banking

A department in a financial institution that provides high-end services to wealthy individuals. Private banking transactions tend to be marked with confidentiality, complex beneficial ownership arrangements, offshore investment vehicles, tax shelters and credit extension services.

Private investment company (PIC)

Also known as a personal investment company, a PIC is a type of corporation that is often established in an offshore jurisdiction with tight secrecy laws to protect the privacy of its owners. In some jurisdictions, an international business company or exempt company is referred to as a private investment company.

Pyramid scheme

See Ponzi scheme.

Red flag

A warning signal that should bring attention to a potentially suspicious situation, transaction or activity.

Regulatory agency

A government entity responsible for supervising and overseeing one or more categories of financial institutions. The agency generally has authority to issue regulations, to conduct examinations, to impose fines and penalties, to curtail activities and, sometimes, to terminate charters of institutions under its jurisdiction. Most financial regulatory agencies play a major role in preventing and detecting money laundering and other financial crimes. Most regulators focus on domestic institutions, but some have the ability to regulate foreign branches and operations of institutions.

Remittance services

Also referred to as giro houses or casas de cambio, remittance services are businesses that receive cash or other funds that they transfer through the banking system to another account. The account is held by an associated company in a foreign jurisdiction where the money is made available to the ultimate recipient.

Reputational risk

The potential that adverse publicity regarding a financial institution's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks and other financial institutions are especially vulnerable to reputational risk because they can become a vehicle for, or a victim of, illegal activities perpetrated by customers. Such institutions may protect themselves through know-your-customer and know-your-employee programs.

Respondent bank

A bank for which another financial institution establishes, maintains, administers or manages a correspondent account.

Risk-based approach

The assessment of the varying risks associated with different types of businesses, clients, accounts and transactions in order to maximize the effectiveness of an anti-money laundering program.

Safe harbor

Legal protection for financial institutions, their directors, officers and employees from criminal and civil liability for breach of any restriction on disclosing information imposed by contract or by any legislative, regulatory or administrative prohibition, if they report their suspicions in good faith to the financial investigation unit (FIU), even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Seize

To prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freeze, a seizure allows the competent authority to take control of specified funds or other assets. The seized assets remain the property of the individual(s) or entity(ies) that held an interest in them at the time of the seizure, although the competent authority will often take over possession, administration or management of the seized assets.

Senior foreign political figure

U.S. term for foreign politically exposed persons. *See politically exposed persons.*

Settlors

People or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trust's assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes done with the assets.

Shell bank

Bank that exists on paper only and that has no physical presence in the country where it is incorporated or licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

Smurfing

A commonly used money laundering method, smurfing involves the use of multiple individuals and/or multiple transactions for making cash deposits, buying monetary instruments or bank drafts in amounts under the reporting threshold. The individuals hired to conduct the transactions are referred to as smurfs. *See structuring.*

Sting operation

Investigative tactic in which undercover officers pose as criminals, sometimes through a front business, to win the confidence of suspected or known criminals to gather information and to obtain evidence of criminal conduct. It is an effective means of identifying criminals, penetrating criminal organizations and identifying tainted property in money laundering and other cases.

Structuring

Illegal act of splitting cash deposits or withdrawals into smaller amounts, or purchasing monetary instruments, to stay under a currency reporting threshold. The practice might involve dividing a sum of money into lesser quantities and making two or more deposits or withdrawals that add up to the original amount. Money launderers use structuring to avoid triggering a filing by a financial institution. The technique is common in jurisdictions that have compulsory currency reporting requirements. *See smurfing.*

Subpoena

Compulsory legal process issued by a court to compel the appearance of a witness at a judicial proceeding, sometimes requiring the witness to bring specified documents. The term can refer to either the process or the actual document that compels the recipient to act.

Suspicious activity

Irregular or questionable customer behavior or activity that may be related to a money laundering or other criminal offense, or to the financing of a terrorist activity. May also refer to a transaction that is inconsistent with a customer's known legitimate business, personal activities or the normal level of activity for that kind of business or account.

Suspicious activity report (SAR)

A government filing required by reporting entities that includes a financial institution's account of a questionable transaction. Many jurisdictions require financial institutions to report suspicious transactions to relevant government authorities such as its FIU on a suspicious activity report (SAR).

Suspicious transaction report (STR)

See suspicious activity report.

Tax haven

Countries that offer special tax incentives or tax avoidance to foreign investors and depositors.

Terrorist financing

The process by which terrorists fund their operations in order to perform terrorist acts. There are two primary sources of financing for terrorist activities. The first involves financial support from countries, organizations or individuals. The other involves a wide variety of revenue-generating activities, some illicit, including smuggling and credit card fraud.

Testimony

Witness' oral presentation, usually under oath, that describes facts known to the witness.

Tipping off

Improper or illegal act of notifying a suspect that he or she is the subject of a suspicious transaction report or is otherwise being investigated or pursued by the authorities.

Trade finance

See letter of credit.

Transparency International (TI)

Berlin-based, nongovernmental organization dedicated to increasing government accountability and curbing both international and national corruption. Established in 1993, TI is active in approximately 100 countries. It publishes corruption news on its website daily and offers an archive of corruption-related news articles and reports. Its Corruption Online Research and Information System, or CORIS, is perhaps the most comprehensive worldwide database on corruption. TI is best known for its annual Corruption Perceptions Index (CPI), which ranks countries by perceived levels of corruption among public officials; its Bribe Payers Index (BPI) ranks the leading exporting countries according to their propensity to bribe. TI's annual Global Corruption Report combines the CPI and the BPI and ranks each country by its overall level of corruption. The lists help financial institutions determine the risk associated with a particular jurisdiction.

Trust

Arrangement among the property owner (the grantor), a beneficiary and a manager of the property (the trustee), whereby the trustee manages the property for the benefit of the beneficiary in accordance with terms set by the grantor.

Trustee

May be a paid professional or company or unpaid person that holds the assets in a trust fund separate from the trustee's own assets. The trustee invests and disposes of the assets in accordance with the settlor's trust deed, taking into consideration any letter of wishes.

Typology

Refers to a money laundering method and is a term used by FATF.

Ultimate beneficial owner (UBO)

See beneficial owner.

U.N. Security Council Resolution 1373 (2001)

Adopted in 2001, the resolution requires member nations to take a series of actions to combat terrorism through the adoption of laws and regulations and the establishment of administrative structures. The resolution also requires member nations to "afford one another the greatest measure of assistance for criminal investigations or criminal proceedings relating to the financing or support of terrorist acts."

Underground banking

See alternative remittance system.

United Nations (U.N.)

An international organization that was established in 1945 by 51 countries committed to preserving peace through cooperation and collective security. Today, nearly every nation in the world belongs to the U.N. *See also Vienna Convention.* The United Nations contributes to the fight against organized crime with initiatives such as the Global Program against Money Laundering (GPML), the key instrument of the U.N. Office of Drug Control and Crime Prevention in this task. Through the GPML, the U.N. helps member states to introduce legislation against money laundering and to develop mechanisms to combat this crime. The program encourages anti-money laundering policy development, monitors and analyzes the problems and responses, raises public awareness about money laundering and acts as a coordinator of joint anti-money laundering initiatives with other international organizations.

Unusual transaction

Transaction that appears designed to circumvent reporting requirements, is inconsistent with the account's transaction patterns or deviates from the activity expected for that type of account.

USA PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law 107-56). Enacted on October 26, 2001, the historic U.S. law brought about momentous changes in the anti-money laundering field, including more than 50 amendments to the Bank Secrecy Act. Title III of the Act, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, contains most, but not all, of its anti-money laundering-related provisions.

Value transfer service

See money transfer service.

Vienna Convention

Convention in 1988 against the Illicit Trade in Narcotic Drugs and Psychotropic Substances. Countries that become parties to the Vienna Convention commit to criminalizing drug trafficking and associated money laundering, and enacting measures for the confiscation of the proceeds of drug trafficking. Article III of the Convention provides a comprehensive definition of money laundering, which has been the basis of much subsequent national legislation.

Virtual currency

A medium of exchange that operates in the digital space that can typically be converted into either a fiat (e.g., government-issued currency) or it can be a substitute for real currency.

Willful blindness

Legal principle that operates in money laundering cases in the U.S. and is defined by courts as the "deliberate avoidance of knowledge of the facts" or "purposeful indifference." Courts have held that willful blindness is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction.

Wire transfer

Electronic transmission of funds among financial institutions on behalf of themselves or their customers. Wire transfers are financial vehicles covered by the regulatory requirements of many countries in the anti-money laundering effort.

Wolfsberg Group

Named after the castle in Switzerland where its first working session was held, the Wolfsberg Group is an association of global financial institutions, including Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse Group, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank and UBS. In 2000, along with Transparency International and experts worldwide, the institutions developed global anti-money laundering guidelines for international private banks. Since then, it has issued several other guidelines on correspondent banking and terrorist financing, among others.

World Bank

The World Bank is a vital source of financial and technical assistance to developing countries. It is not a bank in the usual sense, but is made up of two unique development institutions owned by 184 member countries—the International Bank for Reconstruction and Development (IBRD) and the International Development Association (IDA). Both organizations provide low-interest loans, interest-free credit and grants to developing countries. In 2002, the IMF and the World Bank launched a 12-month pilot program to assess countries' anti-money laundering and counter-terrorist financing measures. The World Bank and the IMF, in conjunction with FATF, developed a common methodology to conduct such assessments based on the FATF's 40 Recommendations.