Money laundering

From Wikipedia, the free encyclopedia

Money laundering is the process of transforming the profits of crime and corruption into ostensibly "legitimate" assets.[1][2] In a number of legal and regulatory systems, however, the term money laundering has become conflated with other forms of financial and business crime, and is sometimes used more generally to include misuse of the financial system (involving things such as securities, digital currencies, credit cards, and traditional currency), including terrorism financing and evasion of international sanctions.[3] Most anti-money laundering laws openly conflate money laundering (which is concerned with *source* of funds) with terrorism financing (which is concerned with *destination* of funds) when regulating the financial system.[4]

Some countries define money laundering as obfuscating sources of money, either intentionally or by merely using financial systems or services that do not identify or track sources or destinations. Other countries define money laundering in such a way as to include money from activity that *would have been* a crime in that country, even if the activity was legal where the actual conduct occurred.[5] There has been some criticism of anti-money laundering laws with some commentators saying that this broad brush of applying money laundering to incidental, extraterritorial, or simply privacy-seeking behaviors is like a financial thoughtcrime.[6]

Contents

History

The concept of money laundering regulations goes back to ancient times and is intertwined with the development of money and banking. Money laundering is first seen with individuals hiding wealth from the state to avoid taxation or confiscation or a combination of both.

In China, merchants around 2000 BCE would hide their wealth from rulers who would simply take it from them and banish them. In addition to hiding it, they would move it and invest it in businesses in remote provinces or even outside China.[7]

Over the millennia many rulers and states imposed rules that would take wealth from their citizens and this led to the development of offshore banking and tax evasion. One of the enduring methods has been the use of parallel banking or Informal value transfer systems such as hawala that allowed people to move money out of the country avoiding state scrutiny.

In the 20th century, the seizing of wealth again became popular when it was seen as an additional crime prevention tool. The first time was during the period of Prohibition in the United States during the 1930s. This saw a new emphasis by the state and law enforcement agencies to track and confiscate money. Organized crime received a major boost from Prohibition and a large source of new funds that were obtained from illegal sales of alcohol.

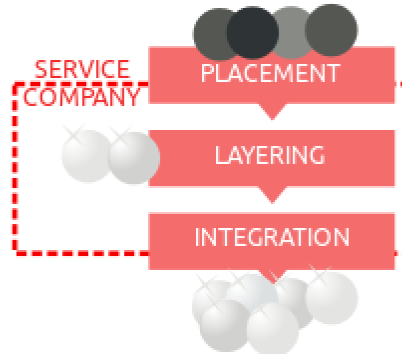
In the 1980s, the war on drugs led governments again to turn to money-laundering rules in an attempt to seize proceeds of drug crimes in order to catch the organizers and individuals running drug empires. It also had the benefit from a law enforcement point of view of turning rules of evidence upside down. Law enforcers normally have to prove an individual is guilty to get a conviction. But with money laundering laws, money can be confiscated and it is up to the individual to prove that the source of funds is legitimate if they want the funds back. This makes it much easier for law enforcement agencies and provides for much lower burdens of proof.

The September 11 attacks in 2001, which led to the Patriot Act in the US and similar legislation worldwide, led to a new emphasis on money laundering laws to combat terrorism financing.[8] The Group of Seven (G7) nations used the Financial Action Task Force on Money Laundering to put pressure on governments around the world to increase surveillance and monitoring of financial transactions and share this information between countries. Starting in 2002, governments around the world upgraded money laundering laws and surveillance and monitoring systems of financial transactions. Anti money laundering regulations have become a much larger burden for financial institutions and enforcement has stepped up significantly. During 2011–2015 a number of major banks faced ever-increasing fines for breaches of money laundering regulations. This included HSBC, which was fined $1.9 billion in December 2012, and BNP Paribas, which was fined $8.9 billion in July 2014 by the US government.[9] Many countries introduced or strengthened border controls on the amount of cash that can be carried and introduced central transaction reporting systems where all financial institutions have to report all financial transactions electronically. For example, in 2006, Australia set up the AUSTRAC system and required the reporting of all financial transactions.[10]

Definition

Money obtained from certain crimes, such as extortion, insider trading, drug trafficking, and illegal gambling is "dirty" and needs to be "cleaned" to appear to have been derived from legal activities, so that banks and other financial institutions will deal with it without suspicion. Money can be laundered by many methods which vary in complexity and sophistication.

Money laundering involves three steps: The first involves introducing cash into the financial system by some means ("placement"); the second involves carrying out complex financial transactions to camouflage the illegal source of the cash ("layering"); and finally, acquiring wealth generated from the transactions of the illicit funds ("integration"). Some of these steps may be omitted, depending upon the circumstances. For example, non-cash proceeds that are already in the financial system would not need to be placed.[11]



Placing "dirty" money in a service company, where it is layered with legitimate income and then integrated into the flow of money, is a common form of money laundering.

According to the United States Treasury Department:

> Money laundering is the process of making illegally-gained proceeds (i.e., "dirty money") appear legal (i.e., "clean"). Typically, it involves three steps: placement, layering, and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the "dirty money" appears "clean."[12]

Methods

Money laundering can take several forms, although most methods can be categorized into one of a few types. These include "bank methods, smurfing [also known as structuring], currency exchanges, and double-invoicing".[13]

- Structuring: Often known as *smurfing*, this is a method of placement whereby cash is broken into smaller deposits of money, used to defeat suspicion of money laundering and to avoid anti-money laundering reporting requirements. A sub-component of this is to use smaller amounts of cash to purchase bearer instruments, such as money orders, and then ultimately deposit those, again in small amounts.[14]

- Bulk cash smuggling: This involves physically smuggling cash to another jurisdiction and depositing it in a financial institution, such as an offshore bank, with greater bank secrecy or less rigorous money laundering enforcement.[15]
- Cash-intensive businesses: In this method, a business typically expected to receive a large proportion of its revenue as cash uses its accounts to deposit criminally derived cash. Such enterprises often operate openly and in doing so generate cash revenue from incidental legitimate business in addition to the illicit cash – in such cases the business will usually claim all cash received as legitimate earnings. Service businesses are best suited to this method, as such businesses have little or no variable costs and/or a large ratio between revenue and variable costs, which makes it difficult to detect discrepancies between revenues and costs. Examples are parking buildings, strip clubs, tanning beds, car washes, and casinos.
- Trade-based laundering: This involves under or overvaluing invoices to disguise the movement of money.[16]
- Shell companies and trusts: Trusts and shell companies disguise the true owner of money. Trusts and corporate vehicles, depending on the jurisdiction, need not disclose their true, beneficial, owner. Sometimes referred to by the slang term *rathole* though that term usually refers to a person acting as the fictitious owner rather than the business entity.[17][18]
- Round-tripping: Here, money is deposited in a controlled foreign corporation offshore, preferably in a tax haven where minimal records are kept, and then shipped back as a foreign direct investment, exempt from taxation. A variant on this is to transfer money to a law firm or similar organization as funds on account of fees, then to cancel the retainer and, when the money is remitted, represent the sums received from the lawyers as a legacy under a will or proceeds of litigation.[19]
- Bank capture: In this case, money launderers or criminals buy a controlling interest in a bank, preferably in a jurisdiction with weak money laundering controls, and then move money through the bank without scrutiny.
- Casinos: In this method, an individual walks into a casino and buys chips with illicit cash. The individual will then play for a relatively short time. When the person cashes in the chips, they will expect to take payment in a check, or at least get a receipt so they can claim the proceeds as gambling winnings.[15]
- Other gambling: Money is spent on gambling, preferably on higher odds. One way to minimize risk with this method is to bet on every possible outcome of some event where there are many possible outcomes and no outcome(s) have short odds – the bettor will lose only the vigorish and will have (a) "winning"

bet(s) that can be shown as the source of money should this be requested. The "losing" bets will remain hidden.

- Real estate: Someone purchases real estate with illegal proceeds and then sells the property.[20] To outsiders, the proceeds from the sale look like legitimate income. Alternatively, the price of the property is manipulated: the seller agrees to a contract that underrepresents the value of the property, and receives criminal proceeds to make up the difference.[17]
- Black salaries: A company may have unregistered employees without a written contract and pay them cash salaries. Dirty money might be used to pay them.[21]
- Tax amnesties: For example, those that legalize unreported assets in tax havens and cash.[22][23]
- Life Insurance Business: Assignment of a policy to unidentified third parties and for which no plausible reasons can be ascertained.[24]

Magnitude

Many regulatory and governmental authorities issue estimates each year for the amount of money laundered, either worldwide or within their national economy. In 1996, the International Monetary Fund estimated that 2–5% of the worldwide global economy involved laundered money. The Financial Action Task Force on Money Laundering (FATF), an intergovernmental body set up to combat money laundering, stated, "Overall, it is absolutely impossible to produce a reliable estimate of the amount of money laundered and therefore the FATF does not publish any figures in this regard."[25] Academic commentators have likewise been unable to estimate the volume of money with any degree of assurance.[11] Various estimates of the scale of global money laundering are sometimes repeated often enough to make some people regard them as factual—but no researcher has overcome the inherent difficulty of measuring an actively concealed practice.

Regardless of the difficulty in measurement, the amount of money laundered each year is in the billions of US dollars and poses a significant policy concern for governments.[11] As a result, governments and international bodies have undertaken efforts to deter, prevent, and apprehend money launderers. Financial institutions have likewise undertaken efforts to prevent and detect transactions involving dirty money, both as a result of government requirements and to avoid the reputational risk involved. Issues relating to money laundering have existed as long as there have been large scale criminal enterprises. Modern anti-money laundering laws have developed along with the modern War on Drugs.[26] In more recent times anti-money laundering legislation is seen as adjunct to the financial crime of terrorist financing in that both crimes usually involve the transmission of funds through the financial system (although money laundering relates to where the money has come *from*, and terrorist financing relating to where the money is going *to*).

Electronic money

In theory, electronic money should provide as easy a method of transferring value without revealing identity as untracked banknotes, especially wire transfers involving anonymity-protecting numbered bank accounts. In practice, however, the record-keeping capabilities of Internet service providers and other network resource maintainers tend to frustrate that intention. While some cryptocurrencies[27] under recent development have aimed to provide for more possibility of transaction anonymity for various reasons, the degree to which they succeed—and, in consequence, the degree to which they offer benefits for money laundering efforts—is controversial.

In 2013, Jean-Loup Richet, a research fellow at ESSEC ISIS, surveyed a new techniques that cybercriminals were using in a report written for the United Nations Office on Drugs and Crime.[28] A common approach was to use a digital currency exchanger service which converted dollars into a digital currency called Liberty Reserve and could be sent and received anonymously. The receiver could convert the Liberty Reserve currency back into cash for a small fee. In May 2013, the US authorities shut down Liberty Reserve charging its founder and various others with money laundering.[29] Another increasingly common way of laundering money is to use online gaming. In a growing number of online games such as Second Life or World of Warcraft, it is possible to convert money into virtual goods, services or virtual cash that can later be converted back into money.[30]

Reverse money laundering

Reverse money laundering is a process that disguises a legitimate source of funds that are to be used for illegal purposes.[31] It is usually perpetrated for the purpose of financing terrorism[32] but can be also used by criminal organizations that have invested in legal businesses and would like to withdraw legitimate funds from official circulation. Unaccounted cash received via disguising financial transactions is not included in official financial reporting and could be used to evade taxes, hand in bribes and pay “under-the-table” salaries.[33] For example, in an affidavit filed 24 March 2014 in United States District Court, Northern California, San Francisco

Division, FBI special agent Emmanuel V. Pascau alleged that several people associated with the Chee Kung Tong organization, and California State Senator Leland Yee, engaged in reverse money laundering activities.

The problem of such fraudulent encashment practices (*obnalichka* in Russian) has become acute in Russia and other countries of the former Soviet Union. The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) reported that the Russian Federation, Ukraine, Turkey, Serbia, Kyrgyzstan, Uzbekistan, Armenia and Kazakhstan have encountered a substantial shrinkage of tax base and shifting money supply balance in favor of cash. These processes have complicated planning and management of the economy and contributed to the growth of the shadow economy.[34]

Combating

Anti-money laundering (AML) is a term mainly used in the financial and legal industries to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report money laundering activities. Anti-money laundering guidelines came into prominence globally as a result of the formation of the Financial Action Task Force (FATF) and the promulgation of an international framework of anti-money laundering standards.[35] These standards began to have more relevance in 2000 and 2001, after FATF began a process to publicly identify countries that were deficient in their anti-money laundering laws and international cooperation, a process colloquially known as "name and shame".[36][37]

An effective AML program requires a jurisdiction to criminalise money laundering, giving the relevant regulators and police the powers and tools to investigate; be able to share information with other countries as appropriate; and require financial institutions to identify their customers, establish risk-based controls, keep records, and report suspicious activities.[38]

Criminalisation

The elements of the crime of money laundering are set forth in the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and Convention against Transnational Organized Crime. It is defined as knowingly engaging in a financial transaction with the proceeds of a crime for the purpose of concealing or disguising the illicit origin of the property from governments.

The role of financial institutions

While banks operating in the same country generally have to follow the same anti-money laundering laws and regulations, financial institutions all structure their anti-money laundering efforts slightly differently.[39] Today, most financial institutions globally, and many non-financial institutions, are required to identify and report transactions of a suspicious nature to the financial intelligence unit in the respective country. For example, a bank must verify a customer's identity and, if necessary, monitor transactions for suspicious activity. This is often termed as "know your customer". This means knowing the identity of the customer and understanding the kinds of transactions in which the customer is likely to engage. By knowing one's customers, financial institutions can often identify unusual or suspicious behaviour, termed anomalies, which may be an indication of money laundering.[40]

Bank employees, such as tellers and customer account representatives, are trained in anti-money laundering and are instructed to report activities that they deem suspicious. Additionally, anti-money laundering software filters customer data, classifies it according to level of suspicion, and inspects it for anomalies. Such anomalies include any sudden and substantial increase in funds, a large withdrawal, or moving money to a bank secrecy jurisdiction. Smaller transactions that meet certain criteria may also be flagged as suspicious. For example, structuring can lead to flagged transactions. The software also flags names on government "blacklists" and transactions that involve countries hostile to the host nation. Once the software has mined data and flagged suspect transactions, it alerts bank management, who must then determine whether to file a report with the government.

Value of enforcement costs and associated privacy concerns

The financial services industry has become more vocal about the rising costs of anti-money laundering regulation and the limited benefits that they claim it brings.[41] One commentator wrote that "[w]ithout facts, [anti-money laundering] legislation has been driven on rhetoric, driving by ill-guided activism responding to the need to be "seen to be doing something" rather than by an objective understanding of its effects on predicate crime. The social panic approach is justified by the language used—we talk of the battle against terrorism or the war on drugs".[42] *The Economist* magazine has become increasingly vocal in its criticism of such regulation, particularly with reference to countering terrorist financing, referring to it as a "costly failure", although it concedes that other efforts (like reducing identity and credit card fraud) may still be effective at combating money laundering.[43]

There is no precise measurement of the costs of regulation balanced against the harms associated with money laundering,[44] and given the evaluation problems involved in assessing such an issue, it is unlikely that the effectiveness of terror finance and money laundering laws could be determined with any degree of accuracy.[45] *The Economist* estimated the annual costs of anti-money laundering efforts in Europe and North America at US$5 billion in 2003, an increase from US$700 million in 2000.[46] Government-linked economists have noted the significant negative effects of money laundering on economic development, including undermining domestic capital formation, depressing growth, and diverting capital away from development.[47] Because of the intrinsic uncertainties of the amount of money laundered, changes in the amount of money laundered, and the cost of anti-money laundering systems, it is almost impossible to tell which anti-money laundering systems work and which are more or less cost effective.

Besides economic costs to implement anti-money-laundering laws, improper attention to data-protection practices may entail disproportionate costs to individual privacy rights. In June 2011, the data-protection advisory committee to the European Union issued a report on data protection issues related to the prevention of money laundering and terrorist financing, which identified numerous transgressions against the established legal framework on privacy and data protection.[48] The report made recommendations on how to address money laundering and terrorist financing in ways that safeguard personal privacy rights and data protection laws.[49] In the United States, groups such as the American Civil Liberties Union have expressed concern that money laundering rules require banks to report on their own customers, essentially conscripting private businesses "into agents of the surveillance state".[50]

Many countries are obligated by various international instruments and standards, such as the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, the 2000 Convention against Transnational Organized Crime, the 2003 United Nations Convention against Corruption, and the recommendations of the 1989 Financial Action Task Force on Money Laundering (FATF) to enact and enforce money laundering laws in an effort to stop narcotics trafficking, international organised crime, and corruption. Mexico, which has faced a significant increase in violent crime, established anti-money laundering controls in 2013 to curb the underlying crime issue.[51]

Global organizations

Formed in 1989 by the G7 countries, the FATF is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. The FATF Secretariat is housed at the headquarters of the OECD in Paris. In October 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body that brings together legal, financial, and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. As of 2014 its membership consists of 36 countries and territories and two regional organizations. FATF works in collaboration with a number of international bodies and organizations. [52] These entities have observer status with FATF, which does not entitle them to vote, but permits them full participation in plenary sessions and working groups.[53]

FATF has developed 40 recommendations on money laundering and 9 special recommendations regarding terrorist financing. FATF assesses each member country against these recommendations in published reports. Countries seen as not being sufficiently compliant with such recommendations are subjected to financial sanctions.[54] [55]

FATF's three primary functions with regard to money laundering are:

1. Monitoring members' progress in implementing anti-money laundering measures,
2. Reviewing and reporting on laundering trends, techniques, and countermeasures, and
3. Promoting the adoption and implementation of FATF anti-money laundering standards globally.

The FATF currently comprises 34 member jurisdictions and 2 regional organisations, representing most major financial centres in all parts of the globe.

The United Nations Office on Drugs and Crime maintains the *International Money Laundering Information Network*, a website that provides information and software for anti-money laundering data collection and analysis.[56] The World Bank has a website that provides policy advice and best practices to governments and the private sector on anti-money laundering issues.[57]

Anti-money laundering measures by region

Many jurisdictions adopt a list of specific predicate crimes for money laundering prosecutions, while others criminalize the proceeds of any serious crimes.

Afghanistan

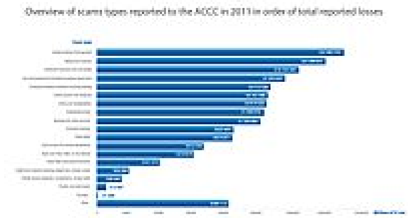
The Financial Transactions and Reports Analysis Center of Afghanistan (FinTRACA) was established as a Financial Intelligence Unit (FIU) under the Anti Money Laundering and Proceeds of Crime Law passed by decree late in 2004. The main purpose of this law is to protect the integrity of the Afghan financial system and to gain compliance with international treaties and conventions. The Financial Intelligence Unit is a semi-independent body that is administratively housed within the Central Bank of Afghanistan (Da Afghanistan Bank). The main objective of FinTRACA is to deny the use of the Afghan financial system to those who obtained funds as the result of illegal activity, and to those who would use it to support terrorist activities.[58]

To meet its objectives, the FinTRACA collects and analyzes information from a variety of sources. These sources include entities with legal obligations to submit reports to the FinTRACA when a suspicious activity is detected, as well as reports of cash transactions above a threshold amount specified by regulation. Also, FinTRACA has access to all related Afghan government information and databases. When the analysis of this information supports the supposition of illegal use of the financial system, the FinTRACA works closely with law enforcement to investigate and prosecute the illegal activity. FinTRACA also cooperates internationally in support of its own analyses and investigations and to support the analyses and investigations of foreign counterparts, to the extent allowed by law. Other functions include training of those entities with legal obligations to report information, development of laws and regulations to support national-level AML objectives, and international and regional cooperation in the development of AML typologies and countermeasures.

Australia

AUSTRAC (Australian Transaction Reports and Analysis Centre) is Australia's financial intelligence unit to combat money laundering and terrorism financing.

Australian responses to money laundering are similar to the majority of western countries. The Financial Transaction Reports Act 1988 (Cth) requires 'cash dealers' to report specific information to the Australian Transaction Reports and Analysis Centre. The purposes of the Financial Transaction Reports Act 1988 (Cth) would be frustrated if accounts could be opened in false names. The Act creates the offence of opening or operating an account in a false name: s 24. It also establishes rigorous procedures that must be followed when opening new accounts when Banking in Australia.The Proceeds of Crime Act 1987 (Cth) imposes criminal penalties on a person who engages in money laundering. The Proceeds of Crime Act 1987 (Cth) attacks the money laundering problem by creating offences and confiscation property.



The Act itself stated its principal objects in a3(1):

(a) to deprive persons of the proceeds of, and benefits derived from the commission of offences.

(b) to provide for the forfeiture of property used in or in connection with the commission of such offences; and

(c) to enable law enforcement authorities to effectively trace such proceeds, benefits and property.[59]

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) is the principal legislative instrument, although there are also offence provisions contained in Division 400 of the *Criminal Code Act 1995* (Cth). Upon its introduction, it was intended that the AML/CTF Act would be further amended by a second tranche of reforms extending to designated non-financial businesses and professions (DNFBPs) including, inter alia, lawyers, accountants, jewellers and real estate agents; however, those further reforms have yet to be progressed.

AUSTRAC works collaboratively with Australian industries and businesses in their compliance with anti-money laundering and counter-terrorism financing legislation.

Financial institutions in Australia are required to track significant cash transactions (at least A$10,000.00 or equivalent in physical cash value) that can be used to finance terrorist activities in and outside Australia's borders and report them to AUSTRAC.

Bangladesh

The first anti-money laundering legislation in Bangladesh was the *Money Laundering Prevention Act, 2002*. It was replaced by the *Money Laundering Prevention Ordinance 2008*. Subsequently, the ordinance was repealed by the *Money Laundering Prevention Act, 2009*. In 2012, government again replace it with the *Money Laundering Prevention Act, 2012*[60]

In terms of section 2, "Money Laundering means – (i) knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:- (1) concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or (2) assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence; (ii) smuggling money or property earned through legal or illegal means to a foreign country; (iii) knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or (iv) concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;(v) converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence; (vi) acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence; (vii) performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised; (viii) participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above.[61][62]

To prevent these Illegal uses of money, the Bangladesh government has introduced the Money Laundering Prevention Act. The Act was last amended in the year 2009 and all the financial institutes are following this act. Till today there are 26 circulars issued by Bangladesh Bank under this act. To prevent money laundering, a banker must do the following:

- While opening a new account, the account opening form should be duly filled up by all the information of the customer.
- The KYC must be properly filled.
- The Transaction Profile (TP) is mandatory for a client to understand his/her transactions. If needed, the TP must be updated at the client's consent.
- All other necessary papers should be properly collected along with the National ID card.
- If any suspicious transaction is noticed, the Branch Anti Money Laundering Compliance Officer (BAMLCO) must be notified and accordingly the Suspicious Transaction Report (STR) must be filled out.

- The cash department should be aware of the transactions. It must be noted if suddenly a big amount of money is deposited in any account. Proper documents are required if any client does this type of transaction.
- Structuring, over/ under invoicing is another way to do money laundering. The foreign exchange department should look into this matter cautiously.
- If any account has a transaction over 1 million taka in a single day, it must be reported in a cash transaction report (CTR).
- All bank officials must go through all the 26 circulars and use them.

Canada

In 1991, the Proceeds of Crime (Money Laundering) Act was brought into force in Canada to give legal effect to the former FATF Forty Recommendations by establishing record keeping and client identification requirements in the financial sector to facilitate the investigation and prosecution of money laundering offences under the Criminal Code and the Controlled Drugs and Substances Act.[63]

In 2000, the Proceeds of Crime (Money Laundering) Act was amended to expand the scope of its application and to establish a financial intelligence unit with national control over money laundering, namely FINTRAC.[63]

In December 2001, the scope of the Proceeds of Crime (Money Laundering) Act was again expanded by amendments enacted under the Anti-Terrorism Act with the objective of deterring terrorist activity by cutting off sources and channels of funding used by terrorists in response to 9/11. The Proceeds of Crime (Money Laundering) Act was renamed the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.[63]

In December 2006, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act was further amended, in part, in response to pressure from the FATF for Canada to tighten its money laundering and financing of terrorism legislation. The amendments expanded the client identification, record-keeping and reporting requirements for certain organizations and included new obligations to report attempted suspicious transactions and outgoing and incoming international electronic fund transfers, undertake risk assessments and implement written compliance procedures in respect of those risks.[63]

The amendments also enabled greater money laundering and terrorist financing intelligence-sharing among enforcement agencies.[63]

In Canada, casinos, money service businesses, notaries, accountants, banks, securities brokers, life insurance agencies, real estate salespeople and dealers in precious metals and stones are subject to the reporting and record keeping obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

European Union

The fourth and latest iteration of the EU's anti-money laundering directive (AMLD IV) was published on 5 June 2015, after clearing its last legislative stop at the European Parliament. The new directive brings the EU's anti-money laundering laws more in line with the US's, which is welcome news for financial institutions that are operating in both jurisdictions.[64]

Lack of harmonization in AML requirements between the US and EU has complicated the compliance efforts of global institutions that are looking to standardize the Know Your Customer (KYC) component of their AML programs across key jurisdictions. AMLD IV promises to better align the AML regimes by adopting a more risk-based approach compared to its predecessor, AMLD III.[64]

Certain components of the directive, however, go beyond current requirements in both the EU and US, imposing new implementation challenges on banks. For instance, more public officials are brought within the scope of the directive, and EU member states are required to establish new registries of "beneficial owners" (i.e., those who ultimately own or control each company) which will impact banks. ALMD IV became effective 25 June 2015.[65]

India

In 2002, the Parliament of India passed an act called the Prevention of Money Laundering Act, 2002. The main objectives of this act are to prevent money-laundering as well as to provide for confiscation of property either derived from or involved in, money-laundering.[66]

Section 12 (1) describes the obligations that banks, other financial institutions, and intermediaries have to

> (a) Maintain records that detail the nature and value of transactions, whether such transactions comprise a single transaction or a series of connected transactions, and where these transactions take place within a month.

(b) Furnish information on transactions referred to in clause (a) to the Director within the time prescribed, including records of the identity of all its clients.

Section 12 (2) prescribes that the records referred to in sub-section (1) as mentioned above, must be maintained for ten years after the transactions finished. It is handled by the Indian Income Tax Department.

The provisions of the Act are frequently reviewed and various amendments have been passed from time to time.[67][68]

The recent activity in money laundering in India is through political parties, corporate companies and the shares market. It is investigated by the Enforcement Directorate and Indian Income Tax Department.[69] According to Government of India, out of the total tax arrears of ₹2,480 billion (US$39 billion) about ₹1,300 billion (US$20 billion) pertains to money laundering and securities scam cases.[70]

Bank accountants must record all transactions over Rs. 1 million. Bank accountants must maintain this records for 10 years. Banks also must make cash transaction reports (CTRs) and suspicious transaction reports over RS. 1 million within 7 days of doubt. They must submit their reports to the Enforcement Directorate and income tax department.

Singapore

Singapore's legal framework for combating money laundering is contained in a patchwork of legal instruments[71], the main elements of which are:

- The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA).[72] This statute criminalises money laundering and imposes the requirement for persons to file suspicious transaction reports (STRs) and make a disclosure whenever physical currency or goods exceeding S$20,000 are carried into or out of Singapore.

- The Mutual Assistance in Criminal Matters Act (MACMA).[73] This statute sets out the framework for mutual legal assistance in criminal matters.
- Legal instruments issued by regulatory agencies (such as the Monetary Authority of Singapore (MAS)[74], in relation to financial institutions (FIs)) imposing requirements to conduct customer due diligence (CDD).[75]

The term ‘money laundering’ is not used as such within the CDSA. Part VI of the CDSA criminalises the laundering of proceeds generated by criminal conduct and drug tracking via the following offences:

- The assistance of another person in retaining, controlling or using the benefits of drug dealing or criminal conduct under an arrangement (whether by concealment, removal from jurisdiction, transfer to nominees or otherwise) [section 43(1)/44(1)].
- The concealment, conversion, transfer or removal from the jurisdiction, or the acquisition, possession or use of benefits of drug dealing or criminal conduct [section 46(1)/47(1)].
- The concealment, conversion, transfer or removal from the jurisdiction of another person’s benefits of drug dealing or criminal conduct [section 46(2)/47(2)].
- The acquirement, possession or use of another person’s benefits of drug dealing or criminal conduct [section 46(3)/47(3)].

United Kingdom

Money laundering and terrorist funding legislation in the UK is governed by four Acts of primary legislation:-

- Terrorism Act 2000[76]
- Anti-terrorism, Crime and Security Act 2001[77]
- Proceeds of Crime Act 2002[78]
- Serious Organised Crime and Police Act 2005[79]
- Money Laundering Regulations 2007
- Money Laundering Regulation, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/599835/Money_Laundering_Regulations_2017_-_FINAL_CONSULTATION_DRAFT_FINAL.pdf)

Money Laundering Regulations are designed to protect the UK financial system, as well as preventing and detecting crime. If a business is covered by these regulations then controls are put in place to prevent it being used for money laundering.

The Proceeds of Crime Act 2002 contains the primary UK anti-money laundering legislation,[80] including provisions requiring businesses within the "regulated sector" (banking, investment, money transmission, certain professions, etc.) to report to the authorities suspicions of money laundering by customers or others.[81]

Money laundering is broadly defined in the UK.[82] In effect any handling or involvement with any proceeds of any crime (or monies or assets representing the proceeds of crime) can be a money laundering offence. An offender's possession of the proceeds of his own crime falls within the UK definition of money laundering.[83] The definition also covers activities within the traditional definition of money laundering, as a process that conceals or disguises the proceeds of crime to make them appear legitimate.[84]

Unlike certain other jurisdictions (notably the US and much of Europe), UK money laundering offences are not limited to the proceeds of serious crimes, nor are there any monetary limits. Financial transactions need no money laundering design or purpose for UK laws to consider them a money laundering offence. A money laundering offence under UK legislation need not even involve money, since the money laundering legislation covers assets of any description. In consequence, any person who commits an acquisitive crime (i.e., one that produces some benefit in the form of money or an asset of any description) in the UK inevitably also commits a money laundering offence under UK legislation.

This applies also to a person who, by criminal conduct, evades a liability (such as a taxation liability)—which lawyers call "obtaining a pecuniary advantage"—as he is deemed thereby to obtain a sum of money equal in value to the liability evaded.[82]

The principal money laundering offences carry a maximum penalty of 14 years' imprisonment.[85]

Secondary regulation is provided by the Money Laundering Regulations 2003,[86] which was replaced by the Money Laundering Regulations 2007.[87] They are directly based on the EU directives 91/308/EEC, 2001/97/EC and 2005/60/EC.

One consequence of the Act is that solicitors, accountants, tax advisers, and insolvency practitioners who suspect (as a consequence of information received in the course of their work) that their clients (or others) have engaged in tax evasion or other criminal conduct that produced a benefit, now must report their suspicions to the authorities (since these entail suspicions of money laundering). In most circumstances it would be an offence, "tipping-off", for the reporter to inform the subject of his report that a report has been made.[88] These provisions do not however require disclosure to the authorities of information received by certain professionals in privileged circumstances or where the information is subject to legal professional privilege. Others that are subject to these regulations include financial institutions, credit institutions, estate agents (which includes chartered surveyors), trust and company service providers, high value dealers (who accept cash equivalent to €15,000 or more for goods sold), and casinos.

Professional guidance (which is submitted to and approved by the UK Treasury) is provided by industry groups including the Joint Money Laundering Steering Group,[89] the Law Society.[90] and the Consultative Committee of Accountancy Bodies (CCAB). However, there is no obligation on banking institutions to routinely report monetary deposits or transfers above a specified value. Instead reports must be made of all suspicious deposits or transfers, irrespective of their value.

The reporting obligations include reporting suspicious gains from conduct in other countries that would be criminal if it took place in the UK.[91] Exceptions were later added for certain activities legal where they took place, such as bullfighting in Spain.[92]

More than 200,000 reports of suspected money laundering are submitted annually to authorities in the UK (there were 240,582 reports in the year ended 30 September 2010. This was an increase from the 228,834 reports submitted in the previous year).[93] Most of these reports are submitted by banks and similar financial institutions (there were 186,897 reports from the banking sector in the year ended 30 September 2010).[93]

Although 5,108 different organisations submitted suspicious activity reports to the authorities in the year ended 30 September 2010, just four organisations submitted approximately half of all reports, and the top 20 reporting organisations accounted for three-quarters of all reports.[93]

The offence of failing to report a suspicion of money laundering by another person carries a maximum penalty of 5 years' imprisonment.[85]

Bureaux de change

All UK *Bureaux de change* are registered with Her Majesty's Revenue and Customs, which issues a trading licence for each location. Bureaux de change and money transmitters, such as Western Union outlets, in the UK fall within the "regulated sector" and are required to comply with the Money Laundering Regulations 2007.[87] Checks can be carried out by HMRC on all Money Service Businesses.

United States

The approach in the United States to stopping money laundering is usually broken into two areas: preventive (regulatory) measures and criminal measures.

Preventive

In an attempt to prevent dirty money from entering the U.S. financial system in the first place, the United States Congress passed a series of laws, starting in 1970, collectively known as the Bank Secrecy Act (BSA). These laws, contained in sections 5311 through 5332 of Title 31 of the United States Code, require financial institutions, which under the current definition include a broad array of entities, including banks, credit card companies, life insurers, money service businesses and broker-dealers in securities, to report certain transactions to the United States Department of the Treasury. Cash transactions in excess of a certain amount must be reported on a currency transaction report (CTR), identifying the individual making the transaction as well as the source of the cash. The law originally required all transactions of US$5,000 or more to be reported, but due to excessively high levels of reporting the threshold was raised to US$10,000. The U.S. is one of the few countries in the world to require reporting of all cash transactions over a certain limit, although certain businesses can be exempt from the requirement.[94] Additionally, financial institutions must report transaction on a Suspicious Activity Report (SAR) that they deem "suspicious", defined as a knowing or suspecting that the funds come from illegal activity or disguise funds from illegal activity, that it is structured to evade BSA requirements or appears to serve no known business or apparent lawful purpose; or that the institution is being used to facilitate criminal activity. Attempts by customers to circumvent the BSA, generally by structuring cash deposits to amounts lower than US$10,000 by breaking them up and depositing them on different days or at different locations also violates the law.[95]

The financial database created by these reports is administered by the U.S.'s Financial Intelligence Unit (FIU), called the Financial Crimes Enforcement Network (FinCEN), located in Vienna, Virginia. The reports are made available to U.S. criminal investigators, as well as other FIU's around the globe, and FinCEN conducts computer assisted analyses of these reports to determine trends and refer investigations.[96]

The BSA requires financial institutions to engage in customer due diligence, or KYC, which is sometimes known in the parlance as know your customer. This includes obtaining satisfactory identification to give assurance that the account is in the customer's true name, and having an understanding of the expected nature and source of the money that flows through the customer's accounts. Other classes of customers, such as those with private banking accounts and those of foreign government officials, are subjected to enhanced due diligence because the law deems that those types of accounts are a higher risk for money laundering. All accounts are subject to ongoing monitoring, in which internal bank software scrutinizes transactions and flags for manual inspection those that fall outside certain parameters. If a manual inspection reveals that the transaction is suspicious, the institution should file a Suspicious Activity Report.[97]

The regulators of the industries involved are responsible to ensure that the financial institutions comply with the BSA. For example, the Federal Reserve and the Office of the Comptroller of the Currency regularly inspect banks, and may impose civil fines or refer matters for criminal prosecution for non-compliance. A number of banks have been fined and prosecuted for failure to comply with the BSA. Most famously, Riggs Bank, in Washington D.C., was prosecuted and functionally driven out of business as a result of its failure to apply proper money laundering controls, particularly as it related to foreign political figures.[98]

In addition to the BSA, the U.S. imposes controls on the movement of currency across its borders, requiring individuals to report the transportation of cash in excess of US$10,000 on a form called Report of International Transportation of Currency or Monetary Instruments (known as a CMIR).[99] Likewise, businesses, such as automobile dealerships, that receive cash in excess of US$10,000 must file a Form 8300 with the Internal Revenue Service, identifying the source of the cash.[100]

On 1 September 2010, the Financial Crimes Enforcement Network issued an advisory on "informal value transfer systems" referencing *United States v. Banki*.[101]

In the United States, there are perceived consequences of anti-money laundering (AML) regulations. These unintended consequences (http://www.natcnc.com/msb/the-unintended-consequences-of-aml-regulations/) include FinCEN's publishing of a list of "risky businesses," which many believe unfairly targeted money service businesses. The publishing of this list and the subsequent fall-out, banks indiscriminately de-risking MSBs, is referred to as Operation Choke Point.

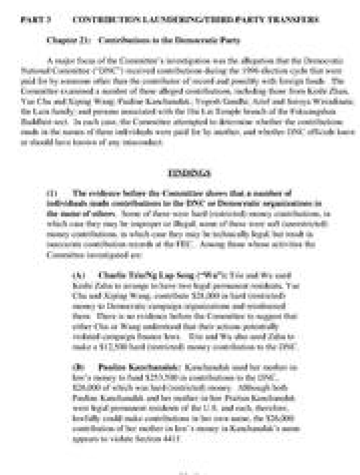
Criminal sanctions

Money laundering has been criminalized in the United States since the Money Laundering Control Act of 1986. The law, contained at section 1956 of Title 18 of the United States Code, prohibits individuals from engaging in a financial transaction with proceeds that were generated from certain specific crimes, known as "specified unlawful activities" (SUAs). The law requires that an individual specifically intend in making the transaction to conceal the source, ownership or control of the funds. There is no minimum threshold of money, and no requirement that the transaction succeeded in actually disguising the money. A "financial transaction" has been broadly defined, and need not involve a financial institution, or even a business. Merely passing money from one person to another, with the intent to disguise the source, ownership, location or control of the money, has been deemed a financial transaction under the law. The possession of money without either a financial transaction or an intent to conceal is not a crime in the United States.[102] Besides money laundering, the law contained in section 1957 of Title 18 of the United States Code, prohibits spending more than US$10,000 derived from an SUA, regardless of whether the individual wishes to disguise it. It carries a lesser penalty than money laundering, and unlike the money laundering statute, requires that the money pass through a financial institution.[102]

According to the records compiled by the United States Sentencing Commission, in 2009, the United States Department of Justice typically convicted a little over 81,000 people; of this, approximately 800 are convicted of money laundering as the primary or most serious charge.[103] The Anti-Drug Abuse Act of 1988 expanded the definition of financial institution to include businesses such as car dealers and real estate closing personnel and required them to file reports on large currency transaction. It required verification of identity of those who purchase monetary instruments over $3,000. The Annunzio-Wylie Anti-Money Laundering Act of 1992 strengthened sanctions for BSA violations, required so called "Suspicious Activity Reports" and eliminated previously used "Criminal Referral Forms", required verification and recordkeeping for wire transfers and established the Bank Secrecy Act Advisory Group (BSAAG). The Money Laundering Suppression Act from 1994 required banking agencies to review and enhance training, develop anti-money laundering examination procedures, review and enhance procedures for referring cases to law enforcement agencies, streamlined the Currency transaction report exemption process, required each Money services business (MSB) to be registered by an owner or controlling person, required every MSB to maintain a list of businesses authorized to act as agents in connection with the financial services offered by the MSB, made operating an unregistered MSB a federal crime, and recommended that states adopt uniform laws applicable to MSBs. The Money Laundering and Financial Crimes Strategy Act of 1998 required banking agencies to develop anti-money laundering training for examiners, required the Department of the Treasury and other agencies to develop a "National Money Laundering Strategy", created the "High Intensity Money Laundering and Related Financial Crime Area" (HIFCA) Task Forces to concentrate law enforcement efforts at the federal, state and local levels in zones where money laundering is prevalent. HIFCA zones may be defined geographically or can be created to address money laundering in an industry sector, a financial institution, or group of financial institutions.[104]

The Intelligence Reform & Terrorism Prevention Act of 2004 amended the Bank Secrecy Act to require the Secretary of the Treasury to prescribe regulations requiring certain financial institutions to report cross-border electronic transmittals of funds, if the Secretary determines that reporting is "reasonably necessary" in "anti-money laundering /combatting financing of terrorists (Anti-Money Laundering/Combating the Financing of Terrorism AML/CFT).

Notable cases



1998 investigation, United States Senate, Contribution Laundering/Third-Party Transfers. Includes investigation of Gandhi Memorial International Foundation.

- Bank of Credit and Commerce International: Unknown amount, estimated in billions, of criminal proceeds, including drug trafficking money, laundered during the mid-1980s.[105]
- Bank of New York: US$7 billion of Russian capital flight laundered through accounts controlled by bank executives, late 1990s.[106]
- Ferdinand Marcos: Unknown amount, estimated at US$10 billion of government assets laundered through banks and financial institutions in the United States, Liechtenstein, Austria, Panama, Netherlands Antilles, Cayman Islands, Vanuatu, Hong Kong, Singapore, Monaco, the Bahamas, the Vatican and Switzerland.[107]
- In December 2012, HSBC: paid a record $1.9 Billion fines for money-laundering hundreds of millions of dollars for drug traffickers, terrorists and sanctioned governments such as Iran.[108] The money-laundering occurred throughout the 2000s.
- In May 2013, Liberty Reserve was seized by United States federal authorities for laundering $6 billion.
- Institute for the Works of Religion: Italian authorities investigated suspected money laundering transactions amounting to US$218 million made by the IOR to several Italian banks.[109]

- Nauru: US$70 billion of Russian capital flight laundered through unregulated Nauru offshore shell banks, late 1990s[110]
- Sani Abacha: US$2–5 billion of government assets laundered through banks in the UK, Luxembourg, Jersey (Channel Islands), and Switzerland, by the president of Nigeria.[111]
- Standard Chartered: paid $330 million in fines for money-laundering hundreds of billions of dollars for Iran. The money-laundering took place in the 2000s and occurred for "nearly a decade to hide 60,000 transactions worth $250 billion".[112]
- Standard Bank: Standard Bank South Africa London Branch – The Financial Conduct Authority (FCA) has fined Standard Bank PLC (Standard Bank) £7,640,400 for failings relating to its anti-money laundering (AML) policies and procedures over corporate and private bank customers connected to politically exposed persons (PEPs).
- In June 2014, BNP Paribas pleaded guilty to falsifying business records and conspiracy, having violated U.S. sanctions against Cuba, Iran, and Sudan. It agreed to pay an $8.9 billion fine, the largest ever for violating U.S. sanctions.[9][113]
- In May 2017, BSI Bank was shut down by the Monetary Authority of Singapore for serious breaches of anti-money laundering requirements, poor management oversight of the bank's operations, and gross misconduct of some of the bank's staff.[114]

In popular culture

Numerous fictional works address money laundering in some depth, e.g.:

- *Better Call Saul*, in which Hector Salamanca uses an ice cream shop and Gus Fring, a chain of chicken restaurants, to launder the proceeds of their drug businesses
- *Breaking Bad*, in which Walter White uses a car wash and Gus Fring, a chain of chicken restaurants and a laundry business, to launder the proceeds of their methamphetamine business
- *Ozark*, in which several characters launder money, such as the protagonist Martin Byrd, who launders money for Camino Del Rio (a Mexican cartel kingpin), and the Snells, long-time Lake of the Ozarks resident criminals who used the Lickety Splitz strip club to launder money until Marty bought it for the same purpose.

See also

- Bank Secrecy Act
- Confiscation
- Currency transaction report
- Customer Identification Program
- Embezzlement
- Financial Action Task Force on Money Laundering
- FBI
- Financial Crimes Enforcement Network
- Global RADAR
- Hawala
- Money trail
- Michael H. O'Keefe
- Office of Foreign Assets Control
- Offshore banking
- Organized crime
- Penny stock scam
- Politically exposed person
- Round-tripping (finance)
- Shell (corporation)
- Terrorist financing
- USA PATRIOT Act
- White-collar crime
- World Bank residual model

References

1. Duhaime, Christine. "What is Laundering? Duhaime's Financial Crime and Anti-Money Laundering Law" (http://www.antimoneylaunderinglaw.com/aml-law-in-canada/what-is-money-laundering). Retrieved 7 March 2014.
2. "Money Laundering — AML-CFT" (https://aml-cft.net/library/money-laundering/). *AML-CFT*. Retrieved 28 May 2017.
3. "Financial Weapons of War, *Minnesota Law Review* (2016)". *ssrn.com*. SSRN 2765010 (https://ssrn.com/abstract=2765010).

4. See for example the Anti-Money Laundering & Counter Terrorism Financing Act 2006 (Australia), the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (New Zealand), and the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap 615) (Hong Kong. See also (for example) guidance on IMF (http://www.imf.org/external/np/leg/amlcft/eng/) and FATF (http://www.fatf-gafi.org/topics/financialinclusion/documents/fatfguidanceonanti-moneylaunderingandterroristfinancingmeasuresandfinancialinclusion.html) websites similarly conflating the concepts.
5. "Anti-Money Laundering – Getting The Deal Through – GTDT" (https://gettingthedealthrough.com/area/50/anti-money-laundering/). *Getting The Deal Through*. Retrieved 28 May 2017.
6. Money Laundering Is Financial Thoughtcrime (http://www.americanbanker.com/bankthink/money-laundering-is-financial-thoughtcrime-1058902-1.html?zkPrintable=1&nopagination=1)
7. Sterling Seagrave (1995). *Lord of the RIM*.
8. Nigel Morris-Cotterill (1999). "A brief history of money laundering" (http://www.countermoneylaundering.com/public/content/brief-history-money-laundering).
9. Protess, Ben & Jessica Silver-Greenberg (30 June 2014). "BNP Paribas Admits Guilt and Agrees to Pay $8.9 Billion Fine to U.S." (https://dealbook.nytimes.com/2014/06/30/bnp-paribas-pleads-guilty-in-sanctions-case/). *The New York Times*. Retrieved 1 July 2014.
10. "AUSTRAC at a glance" (http://www.austrac.gov.au/ar-14-15-austrac-at-a-glance). AUSTRAC. Retrieved 18 August 2016.
11. Reuter, Peter (2004). *Chasing Dirty Money* (http://bookstore.piie.com/book-store//381.html). Peterson. ISBN 978-0-88132-370-2.
12. "History of Anti-Money Laundering Laws" (https://www.fincen.gov/history-anti-money-laundering-laws). United States Department of the Treasury. 30 June 2015. Retrieved 30 June 2015.
13. Lawrence M. Salinger, *Encyclopedia of white-collar & corporate crime: A – I, Volume 1*, page 78, ISBN 0-7619-3004-3, 2005.
14. National Drug Intelligence Center (August 2011). "National Drug Threat Assessment" (http://www.justice.gov/ndic/pubs44/44849/44849p.pdf) (PDF). p. 40. Retrieved 20 September 2011.
15. "National Money Laundering Threat Assessment" (http://www.justice.gov/dea/pubs/pressrel/011106.pdf) (PDF). December 2005. p. 33. Retrieved 3 March 2011.
16. Baker, Raymond (2005). *Capitalism's Achilles Heel*. Wiley.
17. Financial Action Task Force. "Global Money Laundering and Terrorist Financing Threat Assessment" (http://www.fatf-gafi.org/dataoecd/48/10/45724350.pdf) (PDF). Retrieved 3 March 2011.
18. http://www.private-eye.co.uk/registry
19. http://www.private-eye.co.uk/registry
20. http://www.private-eye.co.uk/registry
21. "Underground Economy Issues. Ontario Construction Secretariat" (http://www.iciconstruction.com/resources/industry_publications/underground_economy_issues.cfm).
22. "Tax amnesties turn HMRC into 'biggest money-laundering operation in history' " (http://blogs.telegraph.co.uk/finance/ianmcowie/100011790/tax-amnesties-turn-hmrc-into-biggest-money-laundering-operation-in-history). Retrieved 14 June 2013.
23. "Tax Crimes — AML-CFT" (https://aml-cft.net/library/tax-crimes/). *AML-CFT*. Retrieved 28 May 2017.
24. "Direct Life Insurers - AML/CFT Red Flags — AML-CFT" (https://aml-cft.net/library/direct-life-insurers-amlcft-red-flags/). *AML-CFT*. Retrieved 28 May 2017.

25. Financial Action Task Force. "Money Laundering FAQ" (http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html). Retrieved 2 March 2011.
26. For example, under UK law the first offences created for money laundering both related to the proceeds from the sale of illegal narcotics under the Criminal Justice Act 1988 and then later under the Drug Trafficking Act 1994.
27. "Cryptocurrencies - Real Time Market Data" (https://www.investing.com/crypto/). Investing.com. Retrieved 9 August 2017.
28. Richet, Jean-Loup (June 2013). "Laundering Money Online: a review of cybercriminals methods". arXiv:1310.2368 (https://arxiv.org/abs/1310.2368).
29. Zetter, Kim (May 2013). "Liberty Reserve founder indicted on $6 billion money-laundering charges" (https://www.wired.com/threatlevel/2013/05/liberty-reserve-indicted/). Wired. Retrieved 20 October 2013.
30. Solon, Olivia (October 2013). "Cybercriminals launder money using in-game currencies" (http://www.wired.co.uk/news/archive/2013-10/21/money-laundering-online). Wired. Retrieved 22 October 2013.
31. International Federation of Accountants. "Anti-Money Laundering" (http://www.ifac.org/sites/default/files/publications/files/anti-money-laundering-2n.pdf) (PDF). Retrieved 27 March 2014.
32. Cassella, S.D. (2003). "Reverse money laundering." *Journal of Money Laundering Control*, 7(1): 92-94.
33. Zabyelina, Yuliya (2015). "Reverse money laundering in Russia: Clean cash for dirty ends (http://www.emeraldinsight.com/doi/full/10.1108/JMLC-10-2014-0039)." *Journal of Money Laundering Control*, 18(2): 202-21.
34. EAG (2012). "Money laundering and terrorist financing with use of physical cash and bearer instruments (http://eurasiangroup.org/WGTYP_2012_10_eng.pdf)", 17th Plenary Meeting of the Eurasian Group on Combating Money Laundering and Financing of Terrorism, 28 December, New Delhi.
35. Financial Action Task Force. "About the FATF" (http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html). Retrieved 20 September 2011.
36. Financial Action Task Force. "About the Non-Cooperative Countries and Territories (NCCT) Initiative" (http://www.fatf-gafi.org/document/51/0,3746,en_32250379_32236992_33916403_1_1_1_1,00.html). Retrieved 20 September 2011.
37. "The Global Anti-Money Laundering Regime: A Short Overview, by Richard Horowitz, Cayman Islands Journal, 6 January 2010" (http://www.compasscayman.com/journal/2010/01/06/The-global-anti-money-laundering-regime--a-short-overview). Compasscayman.com. Retrieved 10 November 2013.
38. Financial Action Task Force. "Money Laundering FAQ" (http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html). Retrieved 20 September 2011.
39. "Financial Crime Job Descriptions - FinCrimeJobs.com" (http://amlsource.com/aml-job-descriptions.php).
40. Roth, John; et al. (20 August 2004). "Monograph on Terrorist Financing" (http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Ch4.pdf) (PDF). National Commission on Terrorist Attacks Upon the United States. pp. 54–56. Retrieved 20 September 2011.
41. Ball, Deborah, et al., (22 March 2011). "U.S. Banks Oppose Tighter Money Rules" (https://www.wsj.com/articles/SB10001424052748704355304576214852895407540). *Wall Street Journal*. Retrieved 19 September 2011.
42. *Money Laundering Bulletin*, Issue 154, June 2008, Dr Jackie Harvey (Newcastle Business School

43. "The Lost Trail" (http://www.economist.com/node/5056338?story_id=E1_VDVGPPR). *The Economist*. 20 October 2005. Retrieved 19 September 2011.
44. Levi, Michael & William Gilmore (2002). "Terrorist Finance, Money Laundering and the Rise of Mutual Evaluation: A New Paradigm for Crime Control?". *European Journal of Law Reform*. **4** (2): 337–364.
45. Levi, Michael (May 2010). "Combating the Financing of Terrorism: A History and Assessment of the Control of 'Threat Finance' ". *The British Journal of Criminology*. **50** (4): 650–669. doi:10.1093/bjc/azq025 (https://doi.org/10.1093%2Fbjc%2Fazq025).
46. "Coming clean" (http://www.economist.com.hk/node/3292933). *The Economist*. 14 October 2004.
47. Bartlett, Brent (May 2002). "The Negative Effects of Money Laundering on Economic Development" (http://www.afp.gov.au/~/media/afp/pdf/m/money-laundering-02.ashx). Asian Development Bank. Retrieved 19 September 2011.
48. Article 29 Data Protection Working Party. "Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing" (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf) (PDF). European Commission. Retrieved 18 February 2014.
49. Article 29 Data Protection Working Group. "Opinion 14/2011 Annex: Recommendations" (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186_en_annex.pdf) (PDF). European Commission. Retrieved 18 February 2014.
50. American Civil Liberties Union. "The Surveillance Industrial Complex" (https://www.aclu.org/FilesPDFs/surveillance_report.pdf) (PDF). Retrieved 23 October 2011.
51. Mallen, Patricia (13 February 2013). "In Mexico, Around $10B Every Year Come From Money Laundering, Which Was Not Illegal in 16 Out of 31 States" (http://www.ibtimes.com/mexico-around-10b-every-year-come-money-laundering-which-was-not-illegal-16-out-31-states-1555099). *International Business Times*. Retrieved 12 March 2014.
52. GAFI, FATF (21 July 2017). "FATF Members and Observers" (http://www.fatf-gafi.org/about/membersandobservers/). *www.fatf-gafi.org*.
53. Financial Action Task Force. "Member Country and Observers FAQ" (http://www.fatf-gafi.org/document/5/0,3746,en_32250379_32236869_34310917_1_1_1_1,00.html).
54. "Mission" (http://www.bitcoinfaststart.com/bitcoin-money-laundering/). Retrieved 21 June 2014.
55. "High-risk and non-cooperative jurisdictions" (http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)). *www.fatf-gafi.org*. 23 June 2017. `|first1=` missing `|last1=` in Authors list (help)
56. International Money Laundering Information Network (http://www.imolin.org/imolin/index.html). Retrieved on 21 October 2011.
57. World Bank Financial Market Integrity (http://www.amlcft.org/). Amlcft.org. Retrieved on 21 October 2011.
58. "fintraca.gov.af" (http://fintraca.gov.af). fintraca.gov.af. Retrieved 10 November 2013.
59. Tyree, Alan (1997). *Digital Cash*. Adelaide, Australia: Butterworths. pp. 82, 86. ISBN 0 409 31316 5.
60. "Money Laundering Act 2012 amended" (https://resource.ogrlegal.com/money-laundering-act-2012-amended/). *Resource Portal of OGR Legal*. OGR Legal. Retrieved 2 November 2015.

61. "Laws and Acts" (https://www.bb.org.bd/aboutus/regulationguideline/lawsnacts.php). *Bangladesh Bank*.
62. "মানিলন্ডারিং প্রতিরোধ আইন, ২০১২" (http://bdlaws.minlaw.gov.bd/bangla_pdf_part.php?act_name=&vol=%E0%A7%AA%E0%A7%A8&id=1088).
63. Duhaime, Christine. "AML Legislation in Canada, Duhaime's Financial Crime and Anti-Money Laundering Law" (http://www.antimoneylaunderinglaw.com/aml-law/aml-legislation-in-canada). Retrieved 7 March 2014.
64. "AML global alignment: Two steps forward, one step back" (http://www.pwc.com/en_US/us/financial-services/regulatory-services/publications/assets/aml-global-alignment.pdf) (PDF). *pwc.com*. PwC Financial Services Regulatory Practice, June 2015.
65. "EUR-Lex – 52013PC0045 – EN – EUR-Lex" (http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0045).
66. "Prevention of Money Laundering Act, 2002" (http://fiuindia.gov.in/downloads/PMLA_2002.pdf) (PDF). Financial Intelligence Unit (FIU-IND), Ministry of Finance, India. Retrieved 10 October 2012.
67. "The Prevention of Money Laundering (Amendment) Act, 2005" (http://fiuindia.gov.in/downloads/PMLA_Amendment_2005.pdf) (PDF). Retrieved 10 November 2013.
68. "The Prevention of Money Laundering (Amendment) Act, 2009" (http://fiuindia.gov.in/downloads/PMLA_Amendment_2009.pdf) (PDF). Retrieved 10 November 2013.
69. "ED – functions" (https://web.archive.org/web/20120426044056/http://www.directorateofenforcement.gov.in/functions.html). Archived from the original (http://www.directorateofenforcement.gov.in/functions.html) on 26 April 2012. Retrieved 20 May 2013.
70. "Recovery of Arrears From Hasan Ali Not Possible: Fin Min" (http://www.outlookindia.com/news/article/Recovery-of-Arrears-From-Hasan-Ali-Not-Possible-Fin-Min/782833). Outlook India. Retrieved 6 July 2014.
71. Chan, Eric. "Getting The Deal Through - Anti-Money Laundering" (http://www.shooklin.com/images/publications/2016/July/AML2016-Singapore.pdf) (PDF). Retrieved 28 May 2017.
72. "Singapore Statutes Online - 65A - Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act" (http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:fe3027c5-b366-400e-a6ca-13817cf77e55%20%20Status:inforce%20Depth:0;rec=0;whole=yes#legis). *statutes.agc.gov.sg*. Retrieved 28 May 2017.
73. "Singapore Statutes Online - 190A - Mutual Assistance in Criminal Matters Act" (http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:dc154955-d03e-44c7-bfea-326219fe8da7%20Depth:0%20Status:inforce;rec=0#legis). *statutes.agc.gov.sg*. Retrieved 28 May 2017.
74. Room, Reading. "Regulatory and Supervisory Framework > Anti Money Laundering and Countering the Financing of Terrorism" (http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism.aspx). *www.mas.gov.sg*. Retrieved 28 May 2017.
75. "How to conduct proper customer due diligence (CDD) — AML-CFT" (https://aml-cft.net/conduct-proper-customer-due-diligence-cdd/). *AML-CFT*. 19 March 2017. Retrieved 28 May 2017.
76. "OPSI: Terrorism Act" (http://www.opsi.gov.uk/acts/acts2000/ukpga_20000011_en_1). Retrieved 14 February 2009.
77. "OPSI: Anti-Terrorist Crime & Security Act" (http://www.opsi.gov.uk/Acts/acts2001/ukpga_20010024_en_1). Retrieved 14 February 2009.

78. "OPSI: Proceeds of Crime Act" (http://www.opsi.gov.uk/acts/acts2002/ukpga_20020029_en_1). Retrieved 14 February 2009.
79. "OPSI: Serious Organised Crime and Police Act 2005" (http://www.opsi.gov.uk/acts/acts2005/ukpga_20050015_en_1). Retrieved 14 February 2009.
80. Sections 327 – 340, Proceeds of Crime Act 2002
81. Section 330, Proceeds of Crime Act 2002
82. Section 340, Proceeds of Crime Act 2002
83. Section 329, Proceeds of Crime Act 2002
84. Section 327, Proceeds of Crime Act 2002
85. Section 334, Proceeds of Crime Act 2002
86. "OPSI: Money Laundering Regulations 2003" (http://www.opsi.gov.uk/si/si2003/20033075.htm). Retrieved 14 February 2009.
87. "OPSI: Money Laundering Regulations 2007" (http://www.opsi.gov.uk/si/si2007/uksi_20072157_en_1). Retrieved 14 February 2009.
88. Section 333A, Proceeds of Crime Act 2002
89. "Joint Money Laundering Steering Group" (http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp;jsessionid=aH1DPtXgUly-?d=749). Retrieved 14 February 2009.
90. "Law Society AML advice" (http://www.lawsociety.org.uk/support-services/risk-compliance/anti-money-laundering). Retrieved 14 February 2015.
91. Section 340(2), Proceeds of Crime Act 2002
92. David Winch, "Money Laundering Law Changes" (http://www.accountingevidence.com/documents/articles/Money%20laundering%20law%20changes.pdf) (2006)
93. The Suspicious Activity Reports Regime Annual Report 2010 published by SOCA
94. "FFIEC website regarding CTR Exemptions" (http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_019.htm). Retrieved 3 November 2014.
95. FinCEN. "Bank Secrecy Act" (http://www.fincen.gov/statutes_regs/bsa/). Retrieved 2 March 2011.
96. FinCEN Mission. "FinCEN mission" (http://www.fincen.gov/about_fincen/wwd/mission.html). Retrieved 2 March 2011.
97. Roth, John; Douglas Greenburg and Serena Willie (2004). "Monograph on Terrorist Financing" (http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf) (PDF): 54–56. Retrieved 2 March 2011.
98. Joseph, Lester; John Roth (September 2007). "Criminal Prosecution of Banks Under the Bank Secrecy Act" (http://www.justice.gov/usao/eousa/foia_reading_room/usab5505.pdf) (PDF). *United States Attorneys' Bulletin*. Retrieved 2 March 2011.
99. "SEC resources" (http://www.sec.gov/about/offices/ocie/amlsourcetool.htm#8). Retrieved 2 March 2011.
100. "IRS web site regarding Form 8300" (https://www.irs.gov/businesses/small/article/0,,id=148857,00.html). Retrieved 2 March 2011.
101. "Informal Value Transfer Systems", Financial Crimes Enforcement Network, 1 September 2010 (http://www.fincen.gov/statutes_regs/guidance/html/FIN-2010-A011.html)
102. Cassella, Stefan (September 2007). "Money Laundering Laws" (http://www.justice.gov/usao/eousa/foia_reading_room/usab5505.pdf) (PDF). *United States Attorneys' Bulletin*: 21–34. Retrieved 2 March 2011.
103. "US Sentencing Commission Date, 2009" (http://www.ussc.gov/Data_and_Statistics/Federal_Sentencing_Statistics/State_District_Circuit/2009/1c09.pdf) (PDF). 2009. Retrieved 2 March 2011.
104. US Dept Treasury. "What is a HICFA?" (http://www.fincen.gov/law_enforcement/hifca/index.html#map_hifca). *Financial Crimes Enforcement Network*. Retrieved 6 March 2014.

105. "BCCI's Criminality" (http://www.globalsecurity.org/intell/library/congress/1992_rpt/bcci/04crime.htm). Globalsecurity.org. Retrieved 3 March 2011.
106. O'Brien, Timothy L. (9 November 2005). "Bank of New York Settles Money Laundering Case" (https://www.nytimes.com/2005/11/09/business/09bank.html). *New York Times*. Retrieved 3 March 2011.
107. Dunlap, David W. (13 January 1991). "Commercial Property: The Bernstein Brothers; A Tangled Tale of Americas Towers and the Crown" (https://www.nytimes.com/1991/01/13/realestate/commercial-property-bernstein-brothers-tangled-tale-americas-towers-crown.html). The New York Times. Retrieved 12 June 2010.
108. "HSBC to Pay Record Fine to Settle Money-Laundering Charges" (https://dealbook.nytimes.com/2012/12/11/hsbc-to-pay-record-fine-to-settle-money-laundering-charges/). *New York Times*. 11 December 2012. Retrieved 24 January 2013.
109. Josephine McKenna (7 December 2009). "Vatican Bank reported to be facing money-laundering investigation" (http://www.timesonline.co.uk/tol/news/world/europe/article6946507.ece). The Times. Retrieved 12 June 2010.
110. Hitt, Jack (10 December 2000). "The Billion Dollar Shack" (https://www.nytimes.com/2000/12/10/magazine/the-billion-dollar-shack.html). *The New York Times*. Retrieved 3 March 2011.
111. "Sani Abacha" (http://www.assetrecovery.org/kc/node/52f770df-a33e-11dc-bf1b-335d0754ba85.0;jsessionid=741FC522C872AFE4D5D201D4EEBB472F). Asset Recovery Knowledge Center. Retrieved 3 March 2011.
112. "Standard Chartered to Pay $330 Million to Settle Iran Money Transfer Claims" (https://dealbook.nytimes.com/2012/12/06/standard-chartered-to-pay-u-s-330-million-to-settle-iran-laundering-claims/). *New York Times*. 6 December 2012. Retrieved 24 January 2013.
113. "FBI — Bank Guilty of Violating U.S. Economic Sanctions" (https://web.archive.org/web/20140715004002/http://www.fbi.gov/news/stories/2014/july/bank-guilty-of-violating-u.s.-economic-sanctions/). Fbi.gov. Archived from the original (https://www.fbi.gov/news/stories/2014/july/bank-guilty-of-violating-u.s.-economic-sanctions/) on 15 July 2014. Retrieved 14 July 2014.
114. "Singapore BSI Bank ordered to shut down — AML-CFT" (https://aml-cft.net/singapore-bsi-bank-ordered-to-shut-down/). *AML-CFT*. 25 September 2016. Retrieved 28 May 2017.

External links

- Money laundering (https://dmoztools.net/Society/Crime/Research/Money_Laundering/) at DMOZ
- UNODC on money-laundering and countering the financing of terrorism (http://www.unodc.org/unodc/en/money-laundering/index.html): profile from the United Nations Office on Drugs and Crime
- Financial Market Integrity Unit (http://www.worldbank.org/amlcft/) of the World Bank
- International Narcotics Control Strategy Report (https://www.state.gov/j/inl/rls/nrcrpt/) (INCSR), annual report issued by the United States Department of State in March every year (prepared by Bureau of International Narcotics and Law Enforcement Affairs) on country money laundering risk