BIG DATA
A Twenty-First
Century Arms Race

CHAPTER 5

Big Data: Mitigating Financial Crime Risk

Miren B. Aparicio

Miren B. Aparicio

Counsel and Senior Consultant, The World Bank Global Practice

Financial crime legislation seeks to enhance transparency in financial transactions and restrict or prevent criminals from using banks and other non-financial sector entities to launder money. Financial integrity laws help prevent money laundering, terrorist financing, bribery, and corruption.[243] Big data is used to comply with regulatory obligations and fight financial crime.

The effectiveness in fighting financial crime is often hindered by the quality and quantity of available data and by financial integrity regulatory asymmetry across jurisdictional boundaries. There are also tensions between the principles that stand behind the rights of transparency and security in financial integrity laws versus data privacy in international data flows.

On the one hand, financial crime legislation requires banks[244] to collect information about who is and who controls any customer (Know Your Customer, or KYC, obligations), employee, or vendor at the beginning of a legal relationship and on an ongoing basis. There are even recordkeeping obligations after the relationship has ended. To fulfill their regulatory requirements, banks need to obtain and analyze comprehensive and quality data from their customers and screen them against sanctions lists provided by authorities, for each country in which the bank operates.

On the other hand, data privacy laws could hinder banks' ability to use big data to fight financial crime. Data privacy laws threaten global banks' ability to adhere to their duty to know their clients and beneficial owners when operating across borders if they make it more difficult for banks to

[243] Anti-money laundering (AML), counter-terrorist financing (CTF), and anti-bribery and anti-corruption laws (ABAC) will be jointly referred to as "financial integrity laws" or "financial crime laws", with main focus on "AML laws" in this chapter.

[244] The term "banks" will be used broadly in this chapter and include financial services firms, such as banks, brokers, or dealers in securities; mutual funds; and futures commission merchants and introducing brokers in commodities.

acquire this information or impede international data flows.[245] Data privacy rules are nevertheless important. Anytime an organization collects customer data, it must ensure that it complies with privacy rules, and preserves private data from cyberattacks.

Global data, which are essential to fighting crime and terrorism, cannot be processed without technology. Data analytics tools augment the ability to analyze data, which was previously structured by automated systems. However, technological tools are only as good as the underlying data they analyze, which is why accurate and quality data are essential. Mining big data is a critical component of an effective anti-money laundering program, and involves extracting and analyzing data that are both structured and unstructured and that reside both in-house and externally. As a result, for analytics tools to effectively mitigate financial crime risks, privacy laws should include exemptions for transparency and security purposes, which should be agreed upon at a global level.

This chapter analyzes the international transparency standards by the Financial Action Task Force (FATF) and the Basel Committee of Banking Supervision. It also analyzes the trends in financial crime laws in the United States and the European Union (commonly considered reference legislation), as well as the regulatory gaps that might be exploited by "bad actors." It then examines the data analytics tools used by the financial sector, its supervisors, and governments to process big data and fight financial crime. Finally, it explores technology innovation (fintech/regtech, smart contracts, and distributed ledgers technologies), and new opportunities for collaboration between the private and public sectors to manage evolving threats.

What Laws and Regulations Are in Place to Help Mitigate Risks?

Criminal activities know no boundaries, so it is important to look beyond the jurisdictional competences of supervisors and law enforcement authorities and promote international cooperation. To make it more difficult for criminals to integrate funds into the financial system, banks are required by national laws to analyze and process data from clients and their transactions that move money across borders. The occasional gaps, which are exploited by criminals, arise from the regulatory asymmetry in the implementation of the FATF 2012 recommendations, and their lack of enforcement at a global level.

International Guidelines

The Financial Action Task Force is the international anti-money laundering (AML) standard-setting body, which was established in response to mounting concern over money laundering by the G7 at the Paris summit in 1989.[246] Hosted by the Organisation for Economic Co-operation and Development (OECD), FATF issued its first round of recommendations in 1990. The recommendations are not bulletproof: Not all FATF members (currently thirty-five countries and two international organizations) criminalize money-laundering offenses or specify which crimes can serve as predicates for money laundering prosecutions. Moreover, the recommendations do not have the force of law.[247] However, they have become the world's blueprint for effective national and international controls for combating money laundering and terrorism financing, even more after the events of September 11, 2001.[248]

The Basel Committee on Banking Supervision, established in 1974 by central bank governors, promotes sound supervisory standards worldwide. In 1988, the Basel Committee set up principles for effective banking supervision and identified deficiencies in a large number of countries.[249] Even among countries with well-developed financial markets, the extent to which banks follow Know Your Customer rules and employ effective client due diligence practices varies, as noted in the 2001 reference paper *Customer Due Diligence for Banks*.[250] Banks are expected to identify their customers, monitor their accounts to identify transactions that do not conform to normal activity for that customer, investigate red flags, and report suspicious transactions of money laundering to competent authorities. Additional guidelines since 1988, including the "Sound management of risks related to money laundering and financing of terrorism" in 2016, address the need for global banks to adopt a global approach in fighting financial crime, applying a sound KYC program, and employing an automated transaction monitoring

[245] See Customer Due Diligence in section Tools to Mitigate Risk.

[246] "What We Do," FATF, http://www.fatf-gafi.org/about/, accessed January 9, 2017.

[247] Financial Action Task Force (FATF), *The Forty Recommendations and Interpretative Notes*, 2012, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

[248] FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, 2012, updated 2016, 7-9.

[249] Basel Committee on Banking Supervision, *Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering,* 1988, http://www.bis.org/publ/bcbsc137.pdf.

[250] Know Your Customer (KYC) is the term employed by banks to refer to Customer Due Diligence processes. Basel Committee on Banking Supervision, *Customer Due Diligence for Banks*, October 2001, http://www.bis.org/publ/bcbs85.pdf.

system (data analytics tools)[251] to both the parent bank (or head office) and all of its branches and subsidiaries worldwide.[252] This proposal by the Basel Committee for banks of supervising clients' activities at a global level employing data analytics tools is a sound risk management goal to prevent financial crime. However, as the Institute of International Finance points out in a recent study, data privacy laws challenge banks' ability to fulfill this goal and FATF should work to improve the effectiveness of its member states' information sharing regimes.[253]

Anti-Money Laundering (AML) Reference Laws

Recent Trends in EU AML Directives

The first European Union (EU) AML Directive of 1991 was confined to drug trafficking, as defined in the 1988 Vienna Convention.[254] The fourth AML Directive (4AMLD) was adopted in 2015 and needs to be transposed into AML national laws by June 2017. This directive introduces an explicit requirement for companies to maintain adequate, accurate, and current information on their beneficial ownership records.[255] This information must be made readily available to competent authorities, designated entities, and any member of the public who can demonstrate a legitimate interest, upon request. EU member states need to create a central beneficial owners' registry and show that they have taken appropriate steps to identify, assess, understand, and mitigate AML/Counter Terrorist Financing (CTF) risk, including with respect to beneficial ownership information. This will also be achieved by way of a National Risk Assessment to be conducted by each EU member state.

After the Paris terrorist attacks in 2015, the European Commission presented (on February 2, 2016) an action plan to strengthen the fight against terrorist financing.[256] The action plan focuses on two main strands of action: tracing illicit financial flows and preventing terrorists from moving funds or other assets; and disrupting the sources of revenue used by terrorist organizations by targeting their capacity to raise funds.

"After the Paris terrorist attacks in 2015, the European Commission presented an action plan to strengthen the fight against terrorist financing."

The action plan listed a number of concrete measures that were immediately put into practice by the European Commission and laid out a path forward to review existing legislation and propose new legislation. As part of the action plan, the European Commission adopted a proposal to amend the 4AMLD (also referred to as "5AMLD" due to the substantial character of the proposed amendments) in July 2016. The revised directive addresses five tasks: (1) ensuring a high level of safeguards for financial flows from high-risk non-EU countries; (2) enhancing the powers of the EU Financial Intelligence Units (FIUs) and facilitating their cooperation; (3) centralizing national bank and payment account registers or central data retrieval systems in all member states; (4) tackling risks linked to anonymous prepaid instruments (e.g., prepaid cards); and (5) addressing terrorist financing risks linked to virtual currencies.

The European Commission proposed expanding the scope of the revised 4AMLD to include virtual currency exchange platforms and custodian wallet providers. FIUs would be able to have direct access to any information held by any obliged entity (even when the reporting entity has not filed a Suspicious Transaction Report). In addition, EU member states will now be obliged to set up a central registry or mechanism to identify the owners of bank and payment accounts on an automatic basis and FIUs will have direct access to these national registers.

Furthermore, the European Commission's proposal creates a harmonized and enhanced approach across the EU for performing due diligence on high-

[251] Basel Committee on Banking Supervision*, Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, 2016, 6-16.

[252] See also, "General Guidelines on Account Opening and Customer Identification," Basel Committee on Banking Supervision, February 2013, http://www.bis.org/publ/bcbs85annex.htm and Basel Committee on Banking Supervision, *Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, February 2016, http://www.bis.org/bcbs/publ/d353.pdf.

[253] Institute of International Finance, Deploying Regtech Against Financial Crime, March 2017, https://www.iif.com/publication/research-note/deploying-regtech-against-financial-crime

[254] The EU directives harmonize national AML standards and need to be transposed into laws by EU member states; even if they are not transposed, they have a direct effect. See "The Direct Effect of European Law," Eur-Lex, January 14, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14547.

[255] Eur-Lex, *Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing*, May 20, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476157559137&uri=CELEX:32015L0849, accessed January 9, 2017.

[256] European Commission, *Anti-Money Laundering and Counter Terrorist Financing: Stronger Rules to Respond to New Threats*, 2016, http://ec.europa.eu/justice/criminal/document/files/aml-factsheet_en.pdf.

risk non-EU countries. This harmonized list of actions will set minimum requirements to be applied by all EU member states and will encompass a number of checks, including on customers, the purpose and nature of the business relationship, and the source of funds.

The Council of the European Union adopted its negotiating position on December 19, 2016, and the Parliament followed with its position on February 28, 2017.[257] The final text is likely to be agreed to in 2017 by the Council and Parliament, though both institutions have different objectives, with the Parliament focusing on transparency and tax evasion and the Council on terrorist financing.[258]

Finally, the European Commission proposed a package to measure the EU's capacity to fight the financing of terrorism and organized crime, delivering on the commitments made in the action plan against terrorist financing from February 2016. The package includes a proposed directive that would establish the criminalization of money laundering for all member states (with the exception of Denmark and Ireland), a proposed regulation that would implement tighter controls on large cash flows, and a proposed regulation to strengthen the mutual recognition of criminal asset freezing and confiscation orders within the European Union.

Recent Trends in US AML Laws

Enacted in 1970, the Bank Secrecy Act (BSA) is the primary US anti-money laundering regulatory statute. It was followed by the world's first anti-money laundering law, the Money Laundering Control Act of 1986.[259] Motivated by the attacks of September 11, 2001, it was amended by the USA Patriot Act.[260]

In particular, the USA Patriot Act of 2001 AML rules have extraterritorial reach and are especially relevant for correspondent banking relationships. Under Section 311, the Treasury Department has the authority to apply special measures to address primary money laundering concerns related to specific banks in foreign jurisdictions.[261] For instance, in 2005, the Treasury designated Banco Delta Asia in Macau as a "primary money laundering concern" and served the bank with a 311 order because it had facilitated a range of illegal activities for North Korea, including counterfeiting $100 bills and money laundering.[262] Practically overnight, banks throughout the region stopped doing business with the Banco Delta. A ripple effect around the international banking community led to the freezing, scrutiny, and isolation of North Korea from the banking system. This result was remarkable for several reasons: the United States could not have proposed any trade sanctions, since there was no trade with North Korea at the time; Banco Delta did not have US accounts to be frozen; and North Korea was not the subject of any United Nations (UN) measure or sanction.[263] Another recent example is Russia, which would like to see an easing of US sanctions on Western financing for its banks and oil companies, because fewer sanctions could easily boost growth by a percentage point or more by some estimates.[264]

The US Treasury can compel US banks to apply gradual protective measures, from recordkeeping practices to closing correspondent accounts. US banks have to apply special due diligence measures and respond to questions about any client or foreign bank they deal with, including who its owners are and the nature of its regulatory oversight.[265] For any correspondent banking account managed by a US financial institution, the US Treasury can request any

[257] EU Council, *Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC,* December 19, 2016, http://data.consilium.europa.eu/doc/document/ST-15605-2016-INIT/en/pdf.

[258] EU Parliament, *Report on the Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC*, March 2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN

[259] Federal Financial Institutions Examinations Council, *Money Laundering Control Act of 1986*, http://www.ffiec.gov/bsa_aml_infobase/documents/regulations/ml_control_1986.pdf.

[260] US Department of Justice, *The USA Patriot Act: Preserving Life and Liberty*, 2001, https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.

[261] "Special Measures: Overview," *Bank Secrecy Act Anti-Money Laundering Examination Manual*, Section 311 of the USA Patriot Act (2001), which amends the Bank Secrecy Act (1970), https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_031.htm.

[262] Bryan Borrough, "In 'Treasury's War,' Missiles for a Financial Battlefield," *New York Times*, August 31, 2013, http://www.nytimes.com/2013/09/01/business/in-treasurys-war-missiles-for-a-financial-battlefield.html.

[263] Samuel Rubenfeld, "Q&A: Juan Zarate, the author of 'Treasury's War,'" *Wall Street Journal,* September 26, 2013, http://blogs.wsj.com/riskandcompliance/2013/09/26/qa-juan-zarate-author-of-treasurys-war.

[264] Neil Buckley, "Buoyant Putin Still Needs Washington to Cut a Deal on Sanctions," *Financial Times*, December 19, 2016, https://www.ft.com/content/13cbbdca-c76b-11e6-9043-7e34c07b46ef. See also Max Seldom and Courtney Weaver, "Trump to Call Putin as He Considers Lifting Russia Sanctions," *Financial Times*, January 27, 2017, https://www.ft.com/content/581eff4e-e49b-11e6-8405-9e5580d6e5fb.

[265] US Department of Justice, *The USA Patriot Act*, Section 312, http://ithandbook.ffiec.gov/media/resources/3356/con-usa_patriot_act_section_312.pdf.

A woman holds bank notes at Banco Delta Asia in Macau, China. *Photo credit:* Reuters/Paul Yeung.

records regarding the account, even those located outside of the United States, including the identity of each beneficial owner of the foreign bank, unless the bank is publicly traded.[266]

Requirements for banks to know their corporate clients' beneficial owners are also increasing in the United States.[267] The USA Patriot Act had already contemplated requiring beneficial ownership information as part of customer due diligence obligations, but the act did not provide a definition of a beneficial owner, so the identification requirements were unclear.

However, the Bank Secrecy Act passed in May 2016, which will become effective in 2018, will address this issue for companies when a new account is opened.[268] Trusts, on the other hand, do not have beneficial ownership identification requirements under the new legislation.[269] This is a significant gap.

[266] US Department of Justice, *The USA Patriot Act*, Section 319(b) and implementing regulations, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_027.htm.

[267] The final rule (§ 1010.230) released by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) on May 6, 2016, to obtain and record beneficial ownership information will increase the customer due diligence obligations of covered financial institutions, which will have two years to implement the new requirements on beneficial ownership, as part of their obligations under the Bank Secrecy Act in Title 31.

[268] The beneficial ownership definition includes any individual who owns directly or indirectly 25 percent or more of the equity interests of the corporate customer. See Department of the Treasury, Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, 31 CFR Parts 1010, 1020, 1023, et al., https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

[269] Ibid. Covered financial institutions include federal regulated banks and credit unions, mutual funds, brokers and dealers in securities, futures comissions merchants and introducing brokers in commodities.

What Are the Regulatory Gaps?

There is a lack of consistent AML regulations across the global community. The different playing fields of controls internationally, caused by deficient AML laws and often by their lack of enforcement by national authorities, create opportunities for "bad actors" to operate in many jurisdictions; this should be tackled as a global priority. Emerging countries, as recently recommended by the Financial Stability Board (FSB), need stricter bank supervision.[270]

Currently, FATF members (thirty-five countries) do not fully implement the FATF 2012 recommendations, and many countries do not implement them at all. This regulatory asymmetry creates jurisdictional gaps, which are exploited by bad actors. The exclusion of politically exposed persons (PEPs), beneficial owners, and "gatekeepers" of the financial sector (such as lawyers, real estate professionals, and trusts) from transparency requirements is a regulatory gap that threatens the global community, as revealed by the Panama Papers.[271] Virtual currencies and other new businesses can be used by bad actors to move money globally.

Financial Sector Gatekeepers

The FATF recommendations contain AML guidelines for the financial sector's "gatekeepers," including trusts and company services providers, lawyers, real estate professionals, casinos, dealers in precious metals and stones, those in the life insurance sector, and money services businesses.[272] Many of these businesses remain unregulated internationally, with AML laws addressing only the financial sector. Some examples of vulnerabilities are as follows:

Law Firms. The FATF 2016 December report on the United States has called law firms' pooled accounts a vulnerability.[273] Tens of billions of dollars every year move through opaque bank accounts managed by law firms that create a gap in US money-laundering defenses. US law firms protect the confidentiality of their pooled accounts citing attorney-client privilege.

Real Estate. In 2016, the US Treasury's Financial Crimes Enforcement Network (FinCEN) issued several Geographic Targeting Orders (GOTs),[274] which apply to title companies located in six major metropolitan areas in the United States (New York, Miami, Los Angeles County, San Diego County, the San Francisco area, and the county that includes San Antonio, Texas) and require them to identify the beneficial owners of legal entities, partnerships, or representatives that make all-cash purchases of high-end residential real estate. GOTs[275] are valid for 180 days and were renewed on February 24, 2017, for a similar period. FinCEN[276] found that about 30 percent of the transactions were related to a beneficial owner with a previous suspicious activity report. The information obtained confirmed the use of shell companies to launder money through the purchase of luxury real estate in "all-cash" transactions and led to enforcement actions. For instance, in June 2016, the Department of Justice seized more than $1 billion in assets from the 1Malaysia Development Berhad fund. The sovereign wealth fund's embezzled assets were transferred into the United States using shell companies and the client bank accounts of law firms to buy luxury real estate properties in Los Angeles, New York, and London.[277]

Trusts and Bearer Shares Corporations. The Panama Papers leak in 2016 also revealed a serious need to supervise non-financial sector entities (such as trust services companies and law firms), despite previous country assessments by FATF. Two years prior, in June 2014, FATF identified strategic deficiencies in Panama, which expedited the adoption of an AML legislation package. Panama's vulnerability to money laundering was that not all financial and non-financial sectors were subjected to AML regulations and supervision. This was addressed in the new legislation and provided the justification, after some technical assistance, to remove Panama

[270] Caroline Binham, "Stricter Bank Supervision Needed in Developing Nations, Say Policymakers," *Financial Times*, December 19, 2016, https://www.ft.com/content/13cbbdca-c76b-11e6-9043-7e34c07b46ef.

[271] "The Panama Papers: A Torrential Leak," *Economist*, April 9, 2016,http://www.economist.com/news/international/21696497-huge-trove-documents-has-revealed-secrets-offshore-business-presaging-tougher.

[272] FATF, *Risk-Based Approach Guidance for Legal Professionals*, October 23, 2008, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/riskbasedapproachguidanceforlegalprofessionals.html

[273] Rachel Louise Ensign and Serena Ng, "Money Laundering Loophole: Law Firms," *Wall Street Journal*, December 27, 2016, A1 and A6.

[274] US Department of Treasury, "Treasury Announces Key Regulations and Legislation to Counter Money Laundering and Corruption, Combat Tax Evasion," Press Release, May 5, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx.

[275] US Department of Treasury, *Geographic Targeting Order*, February 21, 2017, https://www.fincen.gov/sites/default/files/shared/Real%20Estate%20GTO%20February%202017%20-%20Generic.pdf.

[276] US Department of the Treasury, "FinCEN Renews Real Estate 'Geographic Targeting Orders' to Identify High-End Cash Buyers in Six Major Metropolitan Areas," Press Release, February 23, 2017, https://www.fincen.gov/news/news-releases/fincen-renews-real-estate-geographic-targeting-orders-identify-high-end-cash.

[277] Louise Story, "US to Expand Tracking of Home Purchases by Shell Companies," New York Times, July 27, 2016, http://www.nytimes.com/2016/07/28/us/us-expands-program-to-track-secret-buyers-of-luxury-real-estate.html?_r=0.

from the FATF (grey) list of countries with strategic deficiencies in February 2016.[278] However, the leak of the law firm Mossack Fonseca shortly after (in April 2016) revealed the continued lack of transparency and extended use of shell companies to launder money and evade trade sanctions.[279] It also suggested that FATF international surveillance of AML country frameworks should be strengthened through independent reviews.

A recent US State Department report points to the country's serious AML deficiencies:

> Numerous factors hinder the fight against money laundering, including the existence of bearer share corporations, a lack of collaboration among government agencies, lack of experience with money laundering investigations and prosecutions, inconsistent enforcement of laws and regulations, and a weak judicial system susceptible to corruption and favoritism. Money is laundered via bulk cash and trade by exploiting vulnerabilities at the airport, using commercial cover and free trade zones (FTZs), and exploiting the lack of regulatory monitoring in many sectors of the economy. The protection of client secrecy is often stronger than authorities' ability to pierce the corporate veil to pursue an investigation.[280]

Fintech: Crowdfunding, Online Lending Platforms, P2P Lending

Online lending platforms, peer-to-peer (P2P) lending, and equity crowdfunding—the raising of capital by selling unregistered securities to investors or lenders over the Internet—are rapidly growing industries in the United States, United Kingdom (UK), and China, according to Morgan Stanley.[281] However, Standard and Poor's has raised concerns about the online lending platforms' capacity to comply with key financial regulatory principles and the quality of the data that the platforms keep and on which they base their loan underwriting decisions.

The 2015 FATF report on Emerging Terrorist Financing Risks points to crowdfunding as an alternative way to transfer funds abroad for terrorism finance purposes, citing the FIU of Canada, which has reported several instances "where individuals under investigation for terrorism-related offences, have used crowdfunding websites prior to leaving and/or attempting to leave Canada."[282] Several cases link P2P lending or crowdfunding platforms with terrorism financing. Online lending platforms should screen lenders and investors against designated terrorist and sanctioned entity lists, take steps to detect fake investors, and report suspicious transactions. The questionable due diligence practices of some crowdfunding platforms internationally, combined with regulatory fragmentation, make crowdfunding vulnerable to exploitation by criminals.

In the San Bernardino, California, terrorist attack, in which a married couple killed fourteen people and wounded others, one of the shooters obtained a loan from a peer-to-peer lending site to finance the attack.[283] The problem in this case was not the source of funding (which was legitimate), but the clients' identification and end use of Syed Raheel Farook's loan, which was not to consolidate loans, as he had alleged, but to purchase guns and munition. P2P lending risk lies in the anonymity of these loans, compared with traditional bank loans to a person who has an account with the bank and whose financial activities can be monitored.

Another potential threat is to cybersecurity and identity theft. In October 2015, US telecommunications giant T-Mobile reported a data breach that affected fifteen million customers. The stolen data could be used to create fake lender or investor profiles to launder money. As an example, fake investors (with stolen T-Mobile identities) could crowdfund a sham company that purports to do charitable work abroad. The investors could transfer funds to the company by purchasing (worthless) equity, and the company could transfer the money abroad under the guise of its business.

[278] The Inter-American Development Bank drafted the new AML legislation, and provided technical assistance to Panama to be removed from the FATF grey list "Panamá prepara nueva ley contra el blanqueo de capitals," La Estrella De Panamá, August 12, 2014, http://laestrella.com.pa/economia/panama-prepara-nueva-contra-blanqueo-capitales/23795230.

[279] "The Lesson of the Panama Papers," *The Economist*, April 9, 2016, http://www.economist.com/news/leaders/21696532-more-should-be-done-make-offshore-tax-havens-less-murky-lesson-panama-papers.

[280] US Department of State, *International Narcotics Control Strategy Report, Vol. II*, 2016, http://www.state.gov/j/inl/rls/nrcrpt/2016/vol2/index.htm.

[281] By 2020, Morgan Stanley forecasts online lenders will reach $47 billion, or 16 percent of total US small and medium enterprise (SME) approvals, Smittipon Srethapramote et al., *Global Marketplace Lending: Disruptive Innovation in Financials*, Morgan Stanley, May 19, 2015, http://bebeez.it/wp-content/blogs.dir/5825/files/2015/06/GlobalMarketplaceLending.pdf.

[282] FATF, *Emerging Terrorist Financing Risks*, "Case Study 19: Crowdfunding," October 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf, 31-32.

[283] Darrell Delamaide, "Loan to Terror Couple Challenges Regulators," *USA Today*, December 15, 2015, http://www.usatoday.com/story/money/2015/12/15/shooting-terrorism-online-loans-san-bernardino/77358520/; "FBI Will Investigate San Bernardino Shootings as Terrorist Act," Federal Bureau of Investigation, December 4, 2015, https://www.fbi.gov/news/stories/fbi-will-investigate-san-bernardino-shootings-as-terrorist-act.

Since 2013, in the United States, crowdfunding platforms have been subject to AML requirements.[284] Under Securities and Exchange Commission and Financial Industry Regulatory Authority (FINRA) rules, equity crowdfunding AML programs must comply with Bank Secrecy Act obligations analogous to those applicable to a broker-dealer, including establishing and maintaining effective customer identification on investors; conducting background checks on each officer, director, and holder of 20 percent voting power of the issuer; monitoring and reporting suspicious activity and complying with requests for information from FinCEN and denying access to its services if it believes the issuer or the offering presents a potential for fraud.

Online lending businesses should employ automated tools to detect and prevent AML risks.[285] Similar to online banking, platforms should use compliance intelligence tools to prevent crowdfunding project initiators from secretly raising funds for illicit purposes. A December 2016 Harvard Business School white paper proposed automating the regulatory compliance activities for online lending platforms and creating a concrete regulatory action plan, including a limited national charter.[286]

On December 2, 2016, the Office of the Comptroller of the Currency (OCC) proposed issuing special purpose national bank charters for financial technology (fintech) companies.[287] In March 2017, the OCC issued a licensing manual draft supplement or Fintech Charter[288] for comments. The OCC will consider applications for special purpose national bank licenses from financial technology companies, which operate one of the core banking activities of "paying checks" (broadly referred to as payment systems) or lending money (including any new form of leasing or discounting). The Fintech Charter would require governance and a risk assessment, including AML, among other regulatory requirements and would subject the firms to OCC supervision. Overall, it would make it possible for fintech companies to provide services across the United States.

Fintech companies would be able to voluntarily apply for a national charter and benefit from uniform (federal) regulation and supervision by the OCC. Chartered fintech companies would need to adopt AML risk-mitigation programs and automated tools similar to banks. As the OCC notes, discounting notes, purchasing bank-permissible debt securities, engaging in lease-financing transactions, and making loans are forms of lending money. Similarly, issuing debit cards or engaging in other means of facilitating payments electronically are the modern equivalent of paying checks. The OCC would consider on a case-by-case basis the permissibility of new activities.

Some EU countries, such as the UK and Spain, have specifically regulated crowdfunding, but it is not regulated at the European level—though some other countries consider crowdfunding as an activity covered under the Markets in Financial Instruments Directive.[289] Regarding lending-based crowdfunding, the European Banking Authority recommends that online platforms should, at a minimum, require borrower background checks; have strong AML policies and procedures in place; offer transparent information regarding their directors, stakeholders, and beneficial owners; and have enough technical capacity and expertise to maximize online security.[290]

The World Bank InfoDev study[291] projects that the market value of crowdfunding will be $96 billion by 2025. It also recommends crowdfunding should occur only on portals that are registered with a national regulatory body that oversees securities, or through clearing houses that conduct mandatory background checks for issuers and investors and require auditing and financial disclosures. Very few crowdfunding platforms meet these requirements today globally. In fact, many platforms raise

[284] Equity crowdfunding is regulated by the US Jumpstart Our Business Startups Act ("JOBS Act") Title 301 ("This title may be cited as the "Capital Raising Online While Deterring Fraud and Unethical Non-Disclosure Act of 2012" or the "Crowdfund Act"); Crowdfunding, 78 Fed. Reg. 66428, 66461-65, proposed November 3, 2013, hereinafter "Regulation Crowdfunding."

[285] Zachary Robock, "The Risk of Money Laundering Through Crowdfunding: A Funding Portal's Guide to Compliance and Crime Fighting," Michigan Business Entrepreneurial Law Review, Vol. 4, No. 1 (2014), http://repository.law.umich.edu/mbelr/vol4/iss1/4/.

[286] Karen Gordon Mills and Brayden McCarthy, *The State of Small Business Lending: Innovation and Technology and the Implications for Regulation*, Harvard Business School Working Paper 17-042, 2016, http://www.hbs.edu/faculty/Publication Files/17-042_30393d52-3c61-41cb-a78a-ebbe3e040e55.pdf, 73 and Chapter 6.

[287] Office of the Comptroller of the Currency, *Exploring Special Purpose National Bank Charters for Fintech Companies*, 2016, https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf.

[288] Office of the Comptroller of the Currency, *Evaluating Charter Applications from Financial Technology Companies*, 2017, https://www.occ.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf.

[289] Financial Conduct Authority, *A Review of the Regulatory Regime for Crowdfunding and the Promotion of Non-readily Realizable Securities by Other Media,* February 2015, https://www.fca.org.uk/publication/thematic-reviews/crowdfunding-review.pdf.

[290] European Banking Authority, "EBA recommends convergence of lending-based crowdfunding regulation across the EU*,"* February 26, 2015, https://www.eba.europa.eu/-/eba-recommends-convergence-of-lending-based-crowdfunding-regulation-across-the-eu.

[291] World Bank, *Crowdfunding's Potential for the Developing World*, 2013, http://www.infodev.org/infodev-files/infodev_crowdfunding_study_0.pdf.

questions regarding the identity of issuers and investors and the fragmentation of the regulatory regimes in cross-border sourcing projects.

Remittances and Money Services Businesses

A risk-based approach should guide the regulation of remittance service providers (RSPs) and money services businesses (such as those that issue travelers checks and prepaid cards) at the global level.[292] At this time, RSPs are mostly unregulated and have different business models. However, after September 2001, the FATF Special Recommendations on Terrorist Financing provided that in order to prevent terrorist financing, informal remittance houses should be licensed and comply with risk-based AML regulatory standards that apply to banks.[293] The European Parliament acknowledges the difficulty in implementing FATF recommendations at a global level, as well as the different terminology employed across jurisdictions (also referred to as "money transfer or money service businesses" in Anglo-Saxon legal systems). The Consultative Group to Assist the Poor, housed at the World Bank, recommends a gradual implementation of AML rules that considers the level of maturity of the monetary industry in each country.[294]

RSPs receive cash from their customers that they transfer internationally through the banking system. Data on who sends and receives these payments in foreign countries are often untraceable and criminals frequently use this anonymity to their advantage. For instance, the HSBC Group paid $1.9 billion in fines to US authorities in 2012 for not supervising its RSP clients, which laundered money from drug cartels through its Mexican unit for years.[295] Mexico is the top destination for money transfers from the United States, according to estimates by the World Bank.[296] However, according to the 2009 International Monetary Fund (IMF) country report for Mexico, RSPs are not required to conduct any customer due diligence except for when transactions exceed $10,000.[297]

Since the financial crisis, remittance start-ups[298] have emerged globally using disruptive technologies such as blockchain in direct payments to mobile phones (P2P money transfers) to provide remittance services across borders. While some of them are not regulated, others are. For instance, Coins.ph is a mobile blockchain-based platform connecting over three hundred million unbanked people in Southeast Asia.[299] Blockchain helps Coins.ph facilitate remittances from any country as long as the sender is able to purchase digital currency. Coins.ph is regulated by the central bank of the Philippines (BSP) as a remittance and foreign exchange company. Since the amounts are small, KYC requirements for opening a Coins.ph account are less demanding than opening a bank account. For low-risk individuals' identification purposes, a risk-based approach permits users to take a selfie on their phone while holding a government identity document. Strategic partnerships with banks also allow Coins.ph customers to use automated teller machines (ATMs) by sending a code to their phone without the need to have a bank account or an ATM card.[300]

Virtual Currency Businesses (Exchanges and E-Wallets)

Bitcoin and other virtual currencies embody a value-transfer system that operates like a currency or a commodity, with no issuer or central authority. There are, however, inherent risks that have

[292] See Committee on Payment and Settlement Systems and World Bank, *General Principles for International Remittance Services*, January 2007, http://www.bis.org/cpmi/publ/d76.pdf. "The World Bank Migration Development Brief," Issue No. 21, October 2013, 29; See also, "Let Them Remit," *The Economist*, July 20, 2013, http://www.economist.com/news/middle-east-and-africa/21581995-western-worries-about-money-laundering-are-threatening-economic-lifeline.

[293] FATF, *Special Recommendations on Terrorist Financing*, *2001,* reviewed 2008, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf; see also World Bank, *Guidance Report for the Implementation of the CPSS-World Bank General Principles for National Remittance Services,* Financial Infrastructure Series, 2007, http://www.worldbank.org/en/topic/paymentsystemsremittances/publication/guidance-report-for-the-implementation-of-the-cpss-wb-general-principles-for-international-remittances, 24-26.

[294] European Parliament, "The Impact of Remittances in Developing Countries", p.30 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/deve/dv/remittances_study_/remittances_study_en.pdf

[295] Aruna Viswanatha and Brett Wolf, "HSBC to Pay $1.2 Billion US Fine in Money Laundering Case," Reuters, December 11, 2012, http://www.reuters.com/article/us-hsbc-probe-idUSBRE8BA05M20121211.

[296] Raúl Herández-Coss, *The US–Mexico Remittance Corridor: Lessons on Shifting from Informal to Formal Transfer System,* World Bank Working Paper No. 47, February 2005, http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/US-Mexico_Remittance_Corridor_WP.pdf.

[297] International Monetary Fund, Mexico: Detailed Assessment Report on Anti-Money Laundering and Combating Terrorism, Country Report, 2009, 130, paragraph 146.

[298] Amit, "11 Money Transfer Companies Using Blockchain Technology," Let's Talk Payments, October 23, 2015, https://letstalkpayments.com/11-money-transfer-companies-using-blockchain-technology-2/.

[299] Kate, "19 Bitcoin Remittance Startups That Won't Let the Cryptocurrency Die," Let's Talk Payments, February 5, 2016, https://letstalkpayments.com/19-bitcoin-remittance-startups-that-wont-let-the-cryptocurrency-die/.

[300] Chamber of Digital Commerce, Georgetown University, "Blockchain and Financial Inclusion White Paper", March 2017, p. 18-19, http://finpolicy.georgetown.edu/newsroom/news/center-releases-white-paper-blockchain-and-financial-inclusion

A chain of block erupters used for Bitcoin mining is pictured at the Plug and Play Tech Center in Sunnyvale, California October 28, 2013. A form of electronic money independent of traditional banking, Bitcoins started circulating in 2009 and have since become the most prominent of several fledgling digital currencies. *Photo credit:* Reuters/Stephen Lam.

attracted the attention of regulators. Due to the anonymity afforded by these currencies, criminals are increasingly using virtual currency exchanges and e-wallets to launder money. For instance, a high percentage of illicit financial flows from developing countries are now being transferred through trade-based money-laundering methods to avoid detection. Using virtual currencies in such international transactions makes them almost untraceable.[301]

Bitcoin's protocol, for example, does not verify participants and generates transactions that are not necessarily associated with a real-world identity. It therefore offers a level of anonymity beyond traditional credit and debit cards or online payment systems, such as PayPal. The transactions in blockchain can be tracked, but mixers can be used to hide the transactions history of any client so it becomes easier to launder money without being detected.[302] Also, the transaction records may reside with multiple entities located in different jurisdictions, which makes it difficult for law enforcement to collect information.

[301] Global Financial Integrity, *Illicit Financial Flows from Developing Countries: 2004-2013,* December 2015, http://www.gfintegrity.org/wp-content/uploads/2015/12/IFF-Update_2015-Final-1.pdf.

[302] FATF Report, "Virtual Currencies Key Definitions and Potential AML/CFT Risks", June 2014, p. 6 , http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed.

Criminal abuse of the bitcoin currency has already featured prominently in several high-profile laundering and fraud cases. In 2014, a board member of the nonprofit Bitcoin Foundation was charged with money laundering for allegedly conspiring with a bitcoin exchange operator to sell $1 million in bitcoins to users of the Silk Road black market.[303] That same year, Japan-based Mt. Gox, then the world's largest bitcoin exchange, announced that hackers had stolen $500 million in bitcoins from its poorly guarded system.[304] Japanese prosecutors later charged former Mt. Gox Chief Executive Officer Mark Karpeles with embezzlement, accusing him of stealing $2.66 million from clients.[305]

The emergence of virtual currency exchanges (VCEs) and other related businesses poses new risks described by the FATF 2014 paper. Anyone with an Internet connection can use them to transfer funds across borders, regardless of jurisdiction, while very few countries have issued regulations surrounding their use.[306] The IMF has pointed out that more could be done to help develop an effective international framework for the regulation of virtual currencies.[307]

In the United States, in 2013, FinCEN issued guidance and rulings on when a VCE must register as a money services business and is subject to anti-money laundering and KYC regulations. However, what constitutes an exchange can be unclear. VCEs engage in exchanging virtual currency for "real currency." However, this gets more complicated when private users (who are not regulated) offer on classified websites to sell or buy bitcoins at a premium or a discount, making the transaction anonymous. A Louisiana chiropractor exchanged more than $3 million in money orders through his credit card accounts for bitcoins that he bought on bitcoin exchanges. The reality is that unlicensed bitcoin exchanges[308] have been connected with other illegal activity.

Virtual currency exchanges, which are considered money transfer businesses in the United States, are regulated by states. While some states allow money transmitters to operate without a license, others require one. In 2015, the New York Department of Financial Services issued specific regulations for virtual currency businesses, requiring anyone conducting these activities in New York State to be licensed (Bitlicense) and to implement customer due diligence requirements and AML programs.[309]

Another challenge is supervision. There is no central oversight authority over the virtual currency exchanges or custodian wallet providers (WPs). In the United States, since 2013, VCEs and WPs have been subject to AML supervision by FinCEN at the federal level. In March 2017, the OCC issued a voluntary charter proposal for financial technology companies (Fintech Charter),[310] which would allow them to operate at the federal level under OCC's supervision.[311]

In the European Union, the 5AMLD will aim to harmonize the AML requirements among EU member states for virtual currency exchanges and custodian wallet providers and impose strict limits on prepaid cards.[312] Under the European Commission's proposal to expand the scope of the revised fourth AMLD (or 5AMLD), VCE platforms and WPs would become "obliged entities" and have to implement similar preventive measures and report suspicious transactions. The new directive would also reduce

[303] Emily Flitter, "Prominent Bitcoin Entrepreneur Charged with Money Laundering," Reuters, January 27, 2014, http://www.reuters.com/article/us-usa-bitcoin-arrests-idUSBREA0Q15N20140128.

[304] Yoshifumi Takemoto and Sophie Knight, "Mt. Gox Files for Bankruptcy, Hit with Lawsuit," Reuters, February 28, 2014, http://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228.

[305] Taiga Uranaka, "Prosecutors File Charges against Ex-CEO of Mt. Gox Bitcoin Exchange," Reuters Canada, September 12, 2015, http://ca.reuters.com/article/technologyNews/idCAKCN0RC04620150912.

[306] FATF, *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems,* June 18, 2008, http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingterroristfinancingvulnerabilitiesofcommercialwebsitesandinternetpaymentsystems.html.

[307] Dong He et al., *Virtual Currencies and Beyond: Initial Considerations*, International Monetary Fund, January 2016, SDN/16/03, 36.

[308] Lester Coleman, "Arrests and Prosecutions Reveal Big Vagaries in Bitcoin Selling Regulations," Cryptocoin News, May 23, 2016, https://www.cryptocoinsnews.com/arrests-and-prosecutions-reveal-big-vagaries-in-bitcoin-selling-regulations/.

[309] New York State Department of Financial Services, New York Codes, Rules, and Regulations, Title 23, *Department of Financial Services,* Chapter I. *Regulations of the Superintendent of Financial Services*, Part 200. *Virtual Currencies,* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

[310] US Department of Treasury, "OCC to Consider Fintech Charter Applications, Seeks Comment," Press Release, December 2, 2016, https://www.occ.treas.gov/news-issuances/news-releases/2016/nr-occ-2016-152.html.

[311] Office of the Comptroller of the Currency, *Evaluating Charter Applications From Financial Technology Companies*, Comptroller's Licensing Manual Draft Supplement, March 2017, https://www.occ.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf.

[312] European Commission, *Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC*, July 5, 2016, http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf; see also Samantha Sheen, *"ACAMS, 4AMLD Part 3: Virtual Currency Exchange Platforms, E-Wallet Providers and Pre-Paid Cards,"* Advancing Financial Crime Professionals Worldwide, July 20, 2016, http://www.acams.org/aml-resources/samantha-sheens-blog/eu-proposals-to-bolster-fight-against-financial-crime/.

the exemption regime for anonymous prepaid cards. In its proposal, the European Commission suggested deleting the exemption for prepaid cards used online, lowering the threshold for non-reloadable prepaid cards from $282 (€250) to $169 (€150), and enhancing the powers of FIUs. However, it is still unclear whether the 5AMLD would require uniform licensing or registration for VCEs and WPs, or whether each EU member state may opt for either regime. In any event, as the European Banking Authority's 2016 opinion pointed out, due to the Internet's reach, there are practical difficulties in preventing unlicensed or unregistered entities from providing digital services across borders.[313]

This problem also applies at the global level, due to the Internet's reach, since the majority of virtual currency businesses remain unregulated. The "big three" Chinese VCEs[314] issued statements in February 2017 disallowing withdrawals for a month to upgrade infrastructure and include "self-regulated" anti-money laundering controls, following regulatory pressures from the People's Bank of China. Regulation for VCEs and WPs should be addressed globally, promoting the adoption of AML, cybersecurity, and consumer protection frameworks and automating the monitoring process.[315]

Politically Exposed Persons (PEPs)

PEPs represent a high-risk category of customers for banks, and are subject to enhanced due diligence in many countries. FATF recommendations include the customer identification of both domestic and foreign PEPs. However, many AML national laws only include the obligation to identify international PEPs and often exclude domestic PEPs, which is a significant gap. The United Nations and the World Bank recommend income and asset disclosure regimes for PEPs to prevent corruption and money laundering.[316] The requirement that public officials declare their income and assets already exists in the United States for government employees, General Schedule (GS)-15 and higher.[317]

The challenge for banks in fulfilling their regulatory obligations to identify and monitor PEPs transactions is mainly that public data from official sources are difficult to obtain. Analytical software for client due diligence purposes often includes PEPs information obtained from private and (when available) public sources, media, and the Internet. However, the data contained are often difficult to analyze in cases of a potential name match, since the available information is frequently incomplete. For instance, the Central Intelligence Agency's library database of chiefs of state and cabinet members of foreign governments provides a public list of names but not dates of birth (which should be necessary for financial firms to investigate potential "false positives," i.e., name matches that do not correspond to the same person).[318] In addition, PEPs have found many ways to avoid detection, such as by opening accounts in the names of corporations, trusts, or close family members or associates.[319] The Corruption Perceptions Index published by Transparency International, a nongovernmental organization devoted to combatting corruption, ranks countries by scores.[320] Quality PEPs data should be available as part of the UN Anti-Money Laundering Information Network, which should consider establishing and maintaining a global repository of PEPs.[321] Disclosure requirements on assets before and after leaving office should be required globally as a transparency measure, following the UN's and World Bank's recommendations.[322]

[313] The European Banking Authority has issued further recommendations in its 2016 opinion to adopt a more comprehensive EU regulatory regime for virtual currencies and set up a wall with the financial sector. See European Banking Authority, *Opinion of the European Banking Authority on the EU Commission's Proposal to Bring Virtual Currencies into the Scope of Directive (EU) 2015/849 (4AMLD)*, August 2016, http://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD.

[314] Samburaj Das, "Bitcoin Withdrawals Postponed, to Resume after Regulatory Approval: Chinese Exchanges," Cryptocoin News, March 8, 2017, https://www.cryptocoinsnews.com/bitcoin-withdrawals-postponed-resume-regulatory-approval-chinese-exchanges/.

[315] See Transaction Monitoring section. Financial Industry Regulatory Authority, *Anti-Money Laundering*, Special NASD Notice to Members 02-21, April 2002, http://www.finra.org/sites/default/files/NoticeDocument/p003704.pdf.

[316] World Bank, *Public Office, Private Interests: Accountability through Income and Asset Disclosure,* 2012, https://star.worldbank.org/star/sites/star/files/Public%20Office%20Private%20Interests.pdf, 7-21.

[317] The US Ethics in Government Act of 1978 sets the financial disclosure requirements for members and employees of the government. See Public Citizen, *Personal Financial Disclosure Requirements for Public Officials*, June 2011, https://www.citizen.org/documents/Personal-Financial-Disclosures-June2011.pdf.

[318] CIA Library of Chiefs of State and Cabinet Members of Foreign Governements, https://www.cia.gov/library/publications/world-leaders-1/

[319] World Bank, *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It,* 2011, 11-16.

[320] Transparency International, "Corruption Perceptions Index 2015," 2015, http://www.transparency.org/cpi2015.

[321] See United Nations International Anti-Money Laundering Information Network, "Anti-Money Laundering International Database (AMLID)," www.imolin.org/amlid/index.html.

[322] World Bank, *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It,* 2011

Beneficial Owners

Transparency requirements in AML laws should go beyond the identity of corporate customers to include their controlling interests or beneficial owners; this recommendation aligns with those of FATF. In the United States, the final rule released by FinCEN on May 6, 2016, adds a new obligation for banks to obtain and record beneficial ownership information on their legal entity clients to ensure clear identification of their stakeholders and controlling interests.[323] The Bank Secrecy Act's new beneficial ownership requirements will become effective in 2018, and will create specific reporting duties with respect to each "legal entity customer" when a new account is opened. The beneficial owner is any individual who owns 25 percent of a company or significantly controls, manages, or directs a customer.[324]

The European Union's 4AMLD of 2015, which goes into effect on June 26, 2017, already follows this FATF recommendation. It sets out specific rules on the collection, storing, and access to information on the ultimate beneficial owner of companies.[325] The new definition of a beneficial owner is further specified as a natural person who ultimately has a shareholding, controlling, or ownership interest with over 25 percent of the shares or voting rights in corporate entities, land title ownership included.[326] Although there are notable differences in the positions of the Council and the European Parliament, and depending on the final agreement, the 5AMLD (or revised fourth AMLD) could widen transparency obligations by lowering the threshold below 25 percent, so that more beneficial owners would need to be identified by banks.

The 5AMLD aims to reinforce such transparency obligations by also proposing to create public access by way of compulsory disclosure of certain information on the beneficial ownership of trusts and other passive non-financial entities such as foundations. The 5AMLD needs to be adopted by the European Parliament and Council and negotiators are aiming to agree to it by summer 2017.[327] The revised fourth AMLD is scheduled to be transposed into national law by all EU member states twelve months after publication in the EU's Official Journal.

A recent example exemplifies why oversight of beneficial ownership records must be strengthened. The Financial Conduct Authority and the New York Department of Financial Services fined Deutsche Bank (DB) in 2016 for failures to pick up the beneficial owners of a Russian trading scheme used by offshore clients to launder money in London. The bank shut its investment bank in Russia as a consequence. The offsetting trades consisted of a series of mirror trades. A small broker in Russia bought from DB blue chip shares for rubles, while the same stocks were sold by a British Virgin Island holding company to DB in London for cash in dollars. An internal audit report found around two thousand similar transactions that transferred money out of Russia, bypassing AML controls and involving around $10 billion. The US Department of Justice is examining potential money laundering and sanctions evasion schemes connected to these transactions.[328] The bank has admitted that "the company has so many different technology systems that the gaps between them are open to manipulation."[329]

Tools to Mitigate Risks

The elaboration of customer risk profiles has been recently called the "fifth" pillar[330] of an AML program, due to the substantial changes introduced by the new FinCEN legislation in 2016. The other four pillars are policies, training, compliance, and independent audit functions. A strong customer due diligence program should include the following information about customers: the full identification of a customer and its beneficial owners (for legal entities), development of a "client profile" and transaction activity profiles (or transaction monitoring) in anticipation of the projected customer's activity,

[323] See US Department of the Treasury, Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, FinCEN Rule § 1010.230, Vol. 81, No. 91, May 11, 2016, https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions.

[324] Ibid. Covered financial institutions include federal regulated banks and credit unions, mutual funds, brokers and dealers in securities, futures comissions merchants and introducing brokers in commodities.

[325] Eur-Lex, *Directive (EU) 2015/849*.

[326] Ibid. See definition of beneficial owner in Eur-Lex, *Directive (EU) 2015/*849, Article 3 and Articles 30 and 31.

[327] *EU Parliament, Report on the Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC,* March 2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN

[328] Karen Freifeld and Arno Schuetze, "Deutsche Fined $630 Million for Failures over Russian Money-Laundering," Reuters, Edition United Kingdom, January 31, 2017, http://uk.reuters.com/article/us-deutsche-mirrortrade-probe-idUKKBN15E2SP.

[329] John O'Donnell, "The 'Mirror' Trades That Caught Deutsche in Russian Web," Reuters, January 31, 2017, http://www.reuters.com/article/uk-deutsche-mirrortrade-probe-scheme-idUKKBN15F23D.

[330] "FinCEN's Final Rule to Enhance Customer Due Diligence Requirements for Financial Institutions," Davis Polk & Wardwell, May 31, 2016, https://www.davispolk.com/publications/fincen%E2%80%99s-final-rule-enhance-customer-due-diligence-requirements-financial-institutions/.

"Data profiling techniques can identify data quality issues; ensure standards are fulfilled; reconcile differences; and suggest solutions for identified problems."

the investigation of unusual customer or account activity (including documentation of findings), and suspicious transaction reporting. The client profile refers to the information gathered about a customer at the account opening that is then used to analyze the customer's behavior (client monitoring) and report potential suspicious activities to the competent Financial Intelligence Unit.

Customer Due Diligence

Banks need to obtain information about potential new corporate customers before they open an account. In the case of legal entities, this includes basic information about the company's directors, shareholders, and beneficial owners. In May 2016, FinCEN issued final rules under the Bank Secrecy Act outlining new customer due diligence requirements, which involve developing customer risk profiles and abiding by Know Your Customer rules, which use customer due diligence tools to mitigate the risk of fraud.[331] Due diligence tools are, in practice, used equally by private and public sector entities. By establishing a customer risk management framework, financial institutions can effectively understand the overall risk posed by their clients. Managing customer data is key for an anti-money laundering program, even before a contractual relationship is entered into. The more a bank or a public sector agency knows about its counterparts or clients, the more likely it is that money-laundering and reputational risk abuses can be prevented.

Initially, the banks obtain KYC information from prospective customers through a series of data-gathering interviews and questionnaires before the account is opened. To determine what type of information should be obtained from clients, a group of international banks from the United States and Europe met with the Basel Institute on Governance at the Wolfsberg Group (an association of banks) in Switzerland in 1999.[332] They set up industry standards, known as the Wolfsberg AML Principles, on how to conduct client questionnaires to gather data from them and mitigate risk. These principles complement FATF recommendations with a technical approach to guide banks in customer due diligence rule implementation.[333]

Customer Profiling

Understanding the purpose of a customer relationship helps a bank formulate a risk-based approach to monitoring each customer's activities and detecting unusual behavior. To develop a customer risk profile, a bank analyzes data about the customer's annual income, net worth, domicile, and principal occupation or business, as well as the customer's history of activities with the bank.

Financial institutions continually review data that could update or enhance established customer identification information. The most common issues with customer data relate to missing or inaccurate data.[334] Not capturing comprehensive risk-relevant data that form a customer risk profile could lead to incorrectly evaluating unusual activity. The challenges can be higher in global organizations where information is not easily shared across jurisdictions or remains in silos in business units that do not communicate.[335]

Once data have been collected, the risk posed by the customer needs to be evaluated. Although the rules do not specifically require a system of risk rating, this process creates a consistent definition of risk across a business unit or an institution and eliminates subjective interpretations of risk levels in processes related to customer due diligence or in transaction monitoring. For instance, FINRA[336] has specifically required that online brokers who do not meet their clients in person should maximize the use of electronic databases to verify information about existing or prospective clients and conduct computerized surveillance on account activity to detect unusual or suspicious transactions.[337]

[331] Department of the Treasury, Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, 31 CFR Parts 1010, 1020, 1023, et al., May 2016, https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

[332] Gemma Aiolfi and Hans-Peter Bauer, "The Wolfsberg Group," in Mark Pieth (ed.), *Collective Action: Innovative Strategies to Prevent Corruption*, (Zurich: Dike, 2012), 1-10, http://www.dike.ch/Collective_Action_Pieth.

[333] Wolfsberg Group, "*Wolfsberg Principles for Correspondent Banking,*" 2002, www.wolfsberg-principles.com/corresp-banking.html.

[334] Issues with customer data often include missing data, multiple names in name lines, names in address lines, inconsistent data standards, duplicates, lack of additional customer information, and extract issues.

[335] Rita Gemayel, "Understanding Customer Risk," ACAMS Today, September-November 2016, Vol. 15, No 4, 64-65.

[336] "NASD Provides Guidance to Member Firms Concerning Anti-Money Laundering Compliance Programs Required by Federal Law," Notice to Members, FINRA, 2002, http://www.finra.org/industry/notices/02-21.

[337] Ibid., 7. See FINRA's guidance to online brokers.

In general, banks use automated programs—which are usually based on a risk-scoring model and data-profiling techniques—to perform AML customer due diligence. Risk-scoring models use numeric values to create client profiles and their associated risk categories (i.e., by product, geographic area, customers who operate online only). The risk categories are then combined to give a composite score. A high-risk assessment may indicate a client needs more scrutiny or enhanced due diligence. Data quality should be addressed at system implementation to avoid creating a massive backlog. Advanced compliance systems offer sophisticated data quality solutions to analyze, cleanse, and de-duplicate customer records. Data profiling techniques can identify data quality issues; ensure standards are fulfilled; reconcile differences; and suggest solutions for identified problems. Building client profiles at the beginning of the client relationship and identifying high-risk customers can later help the bank focus its resources on monitoring transactions more accurately and effectively, based on client risk. For instance, FinCEN found that Eurobank's[338] automated system failed to adequately capture numerous transactions related to the same customer. Also, the automated system did not monitor for suspicious activity based on customer risk profiles, or the type and volume of customer transactions.[339]

Sanctions Screening

Before a bank starts doing business with a prospective customer, it must check the customer against published lists of known or suspected terrorists to mitigate the regulatory risk of dealing with sanctioned parties and comply with AML laws. This automated process is called sanctions screening and must be periodically undertaken by banks once a client relationship has been established, at least for each new transaction with a customer. The hundreds of names of individuals and businesses that appear in several lists of sanctioned parties issued by the United Nations, the US government (including the Office of Foreign Assets Control or OFAC List) need to be screened against each bank's customer databases. Global banks should be in a position to simultaneously monitor many sanctions lists issued by several countries, including notably the EU and the UK Treasury consolidated lists.[340]

Because banks cannot rely on manual controls to detect sanctioned parties from their customers' databases, good technological tools and quality structured data on each customer profile play important roles in this effort. For instance, a client name may initially match a sanctions list name (e.g., Pablo Escobar) but a check on the client's date of birth from a passport will reveal that this red flag is just a "false match" or "false positive." Banks use automated sanctions-screening tools, which aggregate all sanctioned entities and individuals. As FINRA points out, "Given the global nature of online brokerage activity, it is essential that online brokers confirm the customer data and review the OFAC List to ensure that customers are not prohibited persons or entities and are not from embargoed countries or regions."[341]

Enterprise risk solutions obtain, analyze, and process data from media, the Internet, and other private and public sources for sanctions-screening purposes. Public sources are necessary to obtain data such as birth certificates or certificates of incorporation from corporate registers. Corporate certificates of incorporation may include the names of directors, stakeholders, and other significant individuals.[342] However, public data lack uniformity across jurisdictions and are challenging for banks to collect on a global level. For instance, official identity documents vary from country to country and are nonexistent in many countries in Africa and Asia. This identity information is key to conducting sanctions-screening and customer-identification programs. In other words, access to public and private information sources is a critical component of the matching process and fundamental to reducing false positives in sanctions-screening processes. Ensuring data quality and their accessibility for AML and security purposes must be seen as a partnership between the private and public sectors, each of which is equally important.[343]

[338] FinCEN, *Assessment of Civil Money Penalty*, in the matter of Eurobank, San Juan, Puerto Rico, US Department of the Treasury, 2010, https://www.fincen.gov/sites/default/files/enforcement_action/AssessmentEurobank.pdf.

[339] Ibid., 4; see also Daniel Nathan and Alma Angotti, *Securities Regulation & Law Report, 44 SRLR 1410, 07/23/2012*, The Bureau of National Affairs, http://www.bna.com.

[340] See Office of Foreign Assets Control, *Specially Designated Nationals and Blocked Persons List*, https://www.treasury.gov/ofac/downloads/sdnlist.pdf; United Nations, *Consolidated United Nations Sanctions List*, https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/consolidated.xsl; European External Action Service, *Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions*, https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions; UK Treasury, *Financial Sanctions: Consolidated List of Targets*, https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.

[341] FINRA Notice, http://www.finra.org/sites/default/files/NoticeDocument/p003704.pdf.

[342] Wolfsberg Group, *Wolfsberg Statement on AML Screening, Monitoring and Searching,* 2009, http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Monitoring_Screening_Searching_Paper_(2009).pdf, 3.

[343] Screening process for PEPs and sanctions requires quality data, including primary name; alias and alternate names; record

KYC Utilities

In correspondent banking relationships, a bank must rely on its foreign bank counterpart's AML controls to detect unwanted clients and process international trade finance or payment transactions on its behalf. Prior to entering into any correspondent relationships between banks, a thorough review of each counterpart's AML control framework is required by AML laws in many countries. For instance, under the USA Patriot Act, a US bank needs to apply enhanced due diligence measures to analyze the risk of doing business with each of its foreign correspondent banking counterparts.[344] In practice, this has created a glut of AML questionnaires being circulated by banks to each and all counterparts as a means of complying with due diligence requirements.

The Wolfsberg Group, an organization composed of an association of private banks, has been collaborating since 2004 with a third-party, private vendor to set up the first international "due diligence repository" for the collection and storage of data, including relevant due diligence information and documentation among member banks. Data on each financial institution at a group level (including its licenses, beneficial owners, corporate governance, directors, managers, and AML controls) are shared among financial entities upon consent, instead of exchanging standard AML questionnaires.[345]

Several providers have developed central identity management facilities or "KYC utilities" with the aim of keeping customer due diligence information in a single repository. Although it has obvious benefits for banks and customers, there is no standardized set of information that should be included in KYC utilities, since there is not a uniform definition of customer due diligence in AML laws and identification documents vary from country to country. Also, data privacy, processing, and localization rules impede the use of information in utilities, and may prevent banks from submitting relevant information to utilities. Utilities are working on solutions for these problems, but a dialogue and coordination with regulatory authorities is essential, since ultimately it could facilitate supervision.

Some KYC utilities are using distributed ledger technology, instead of a single repository, to store client due diligence information. As FINRA points on in a recent report, the responsibility ultimately cannot be transferred to the utility: "While broker-dealers may choose to outsource certain functions to a central utility or a third party on the network, firms need to be aware that they may not outsource their responsibility associated with the performance, or lack thereof, of those functions (see, e.g., "Notice to Members 05-48: Outsourcing.")[346]

SWIFT announced in January 2016 that over two thousand financial institutions in over two hundred countries and territories had signed up for their KYC utility, which maintains standardized sets of data—including KYC information for correspondent banks, fund distributors, and custodians—that can be shared among members.[347]

Supply Chain Management

Automated tools can track vendors and service providers. Due diligence tools help governments and the private sector understand how their supply chains operate and where key suppliers are located. For example, the acquisition of raw materials (e.g., conflict diamonds) can be traced: due diligence tools help provide information on country risk and gaps in transparency by fully mapping supply chains to avoid human trafficking or forced labor. These tools are used by private and public sector entities to comply with public procurement rules, sanctions, or environmental or government export controls regulations.[348] As an example, the Department of Defense and many other US agencies, which have strict procurement rules, may use automated tools similar to those used by banks to track vendors that respond to its requests for proposals.

There are many automated screening tools that analyze data related to background checks on prospective and current employees, contractors, and vendors, especially for criminal history. These are in addition to customer due diligence tools for name screening against sanctions lists and negative news. Employee background checks impede bad actors from accessing company information and systems, thereby preventing potential fraud and regulatory and reputational risks. The Federal Deposit Insurance Corporation has provided specific guidance to the financial sector, recommending a risk-focused approach (higher for managerial

type (individual, entity, vessel); gender; date of birth; age; country; address (country, city, address lines); national ID and passport number.

[344] See *The USA Patriot Act*, Section 312, http://ithandbook.ffiec.gov/media/resources/3356/con-usa_patriot_act_section_312.pdf ,

[345] "International Due Diligence Repository," Wolfsberg International, http://www.wolfsberg-principles.com/diligence.html.

[346] FINRA, Distributed Ledger Technology: Implications of Blockchain for the Securities Industry, January 217, p. 15, http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf

[347] SWIFT, "SWIFT´s KYC Registry Surpasses 2,000 Financial Institutions," January 19, 2016, https://www.swift.com/insights/press-releases/swift_s-kyc-registry-surpasses-2_000-financial-institutions.

[348] US Department of State, *Trafficking in Persons Report*, *Preventing Human Trafficking in Global Supply Chains*, 2015, https://www.state.gov/documents/organization/245365.pdf, 13-33.

A taxi passes a company list showing the Mossack Fonseca law firm at the Arango Orillac Building in Panama City. The International Consortium of Investigative Journalists released a database with information on more than 200,000 offshore entities that are part of the Panama Papers investigation. *Photo credit:* Reuters/Carlos Jasso.

levels) and several background screenings, including fingerprint checks against a criminal database. Some regulations prohibit any person who has been convicted of a crime involving fraud or money laundering from owning or controlling an institution or participating in managerial functions.[349]

Transaction Monitoring

The first challenge for a global bank is identifying the unusual or suspicious transactions within the massive amount of data generated by its global transactions. Big data analytics are essential for detecting illicit activities, which are hidden within layers of multibillion dollar transactions, particularly in trade-related businesses and government programs. Data analytics tools are equally applied by banks for the prevention of money laundering and by government agencies in data intensive fraud investigations.

Big data analytics aggregate data from multiple platforms and should be designed to quickly and accurately identify and flag financial transactions that involve individuals or entities included on watch lists and involved in suspicious transactions. Integrating data from multiple sources—such as linking client email and all available financial transaction data, including clients' financial records, if available—into a single big data platform would increase the accuracy of analytics.

Adopting new cognitive computing systems will increase and enhance the human capacity in the investigation and decision-making process related to clients' suspicious transactions.[350] Intelligent process

[349] Federal Deposit Insurance Corporation, Pre-Employment Background Screening. Guidance on Developing an Effective Pre-Employment Background Screening Process, 2005, https://www.fdic.gov/news/news/inactivefinancial/2005/fil4605.pdf.

[350] Bryan Bell and Robert A. Goldfinger, "Compliance Solutions: Combining Cognitive Computing with Human Intelligence," ACAMS Today, September-November 2016, Vol. 15, No. 4, pg. 50-51.

automation (IPA)[351] is a set of new technologies that combines robotic process automation and machine learning. IPA can replace human effort in processes that involve analyzing and aggregating data from multiple sources. As an example, IPA technologies can be programmed to monitor clients' financial activities and learn from such recognized patterns to detect unusual behavior. In doing so, data analytics tools will become more efficient in detecting patterns of suspicious transactions that may be further analyzed by compliance professionals to detect potential illicit activity.[352]

The Basel Committee's 2016 report recommends automating the monitoring process for banks that are internationally active. Effective techniques for global bank transaction monitoring should combine all client accounts. Transaction monitoring tools, whether developed internally or acquired from vendors, should scan, filter, and analyze customer account activities and data. Such automated tools "must enable the Bank to undergo trend analysis of transaction activity and to identify unusual business relationships and transactions in order to prevent [money laundering]."[353]

Since 2002, FINRA has recommended adopting computerized surveillance tools, jointly with a risk-based review and investigation of alerts, for online brokers and other global firms to detect and report suspicious transactions to law enforcement.[354] The FinCEN fines imposed on Eurobank and Wachovia suggest it would be difficult for US banks with large transaction volumes or international operations to meet FinCEN regulatory expectations for identifying and reporting suspicious transactions by relying only on manual controls. Eurobank relied mostly on manual processes to monitor transactions for suspicious activity.[355] This seemed particularly inadequate to FinCEN, given "the Bank's customer base, geographic risk and business lines, as well as the volume, scope, and types of transactions conducted at the Bank."[356]

Another challenge is setting the appropriate thresholds[357] for monitoring purposes, which often depend on the type of business account and client relationship. In transaction monitoring systems, programming is key. The adequacy of a bank's systems will be tested in an inspection visit or by an independent audit. A review of the number of unusual transactions, the way they are analyzed and documented, and finally the number and quality of suspicious activities filed with FIUs can be very revealing. A very low number of alerts compared with a high number of transactions conducted by a bank may suggest that the setting for the alert programming is wrong, particularly if the business involves high-risk jurisdictions, transactions, or customers. Also, a sound suspicious activity–monitoring program for global banks needs to include all client accounts and transactions across business lines and multiple countries.[358] For instance, in the Wachovia case, FinCEN found that "Wachovia's automated transaction monitoring systems were inadequate to support the volume, scope, and nature of international money transfer transactions conducted by the Bank. . . . The number of alerts or events generated by the Bank's automated transaction systems was capped to accommodate the number of available compliance personnel."[359]

Independent Audits

Compliance reviews and internal audits are independent functions that oversee business units and are the second and third lines of defense of an AML program. As FinCEN in the Wachovia fine noted, there was room for improvement in the independent validation of the audit function as a tool to mitigate risk: "In addition, the monitoring system's programming, methodology, and effectiveness were not independently validated to ensure that the models were detecting potentially suspicious activity."[360]

The volume of regulatory requirements and data involved renders manual compliance inadequate for analyzing customer profiles and account transactions. Data are meaningless unless they are organized in a way that enables people to analyze

[351] Albert Bollard, Elixabete Larrea, Alex Singla, and Rohit Sood, *The Next-Generation Operating Model for the Digital World*, McKinsey & Company, 2017, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-next-generation-operating-model-for-the-digital-world.

[352] George Anadiotis, "Big Data versus Money Laundering: Machine Learning, Applications and Regulation in Finance," ZDNet, http://www.zdnet.com/article/big-data-versus-money-laundering-machine-learning-applications-and-regulation-in-finance/.

[353] Basel Committee on Banking Supervision, *Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, 6.

[354] Financial Industry Regulatory Authority, *Anti-Money Laundering*, Special NASD Notice to Members 02-21.

[355] FinCEN, *Assessment of Civil Money Penalty*, in the matter of Eurobank, San Juan, Puerto Rico.

[356] Ibid.

[357] Nathan and Angotti, "Broker-Dealer AML Transaction Monitoring: The Devil's in the Details."

[358] Ibid.

[359] US Department of the Treasury, Financial Crimes Enforcement Network*, Assessment of Civil Money Penalty*, in the matter of Wachovia Bank*,* No. 2010-1, https://www.fincen.gov/sites/default/files/enforcement_action/100316095447.pdf, 4.

[360] Ibid., 4.

them and make decisions based on the results of those analyses. An independent audit can test the sophistication of data analytics tools, as well as their thresholds and the potential biases in algorithms.[361] The employment of data analytics tools and the quality and frequency of audits to validate such risk management systems can be revealing about the institution and its management's commitment to fighting financial crime. Banks have to employ qualified and experienced audit and compliance staff empowered to investigate suspicious transactions and make independent decisions. In addition, high-quality, independent, and frequent external audits are needed to test controls.

Training Programs

Many AML laws around the world require banks to implement mandatory training programs for their employees as a preventive measure. For instance, the USA Patriot Act requires AML programs to include an ongoing employee training program.[362] A sound training program for global banks should include a practical course focused on how to avoid money laundering and sanctions risks within the parameters of an employee's regular job routine. Its content should include applicable legal requirements and references to policies and procedures but also other fundamental aspects, such as how to recognize vulnerabilities and make the right judgements by showing real examples of good and bad control tests; how suspicious transactions activity is recorded and documented; when and how to raise concerns or seek support from financial crime compliance and risk professionals; and a broader and deeper understanding of the financial crime risks within a business context. Such AML programs need to be risk-based and function-specific—business lines must be able to identify and report suspicious transactions for the AML program to be effective.

Additional Tools to Help Governments and Law Enforcement Manage Evolving Threats

Regtech

Regtech (derived from the words regulation and technology) is often used to explain how technology can help banks and regulators fulfill their regulatory compliance reporting obligations and supervisory duties.[363] Regtech uses digital technologies (including big data analytics, cloud computing, and machine learning) to automate compliance and risk-management processes, facilitate regulatory reporting, and track regulatory changes worldwide. As an example, regtech makes it possible to identify the "one to many" relationship for the first time (i.e., where one control satisfies many regulations, or where a single regulation requires multiple controls). Different forms of technological innovation can facilitate the automation of data reporting from regulatory filings of suspicious transactions (SARs) or currency transaction reports.[364] In particular, they can set up intelligent queries and algorithms to detect SARs. It may also be easier for financial institutions to maintain records for regulators, audits, or inspection visits.[365]

Big data analytics and data science also have wide applications for the private sector and governments to enhance financial crime supervision, particularly in areas such as trade-based money laundering. Data mining, network analysis, and algorithms designed to assess probabilistic measures of suspicious activity in financial transaction data can help with compliance by mining the data related to clients' activities and uncover hidden patterns in the flow of the funds. This could help increase transparency in transactions related to the multibillion dollar global trade and finance industry as well as those in the shadow banking industry, which challenge law enforcement authorities. Both types of transactions are highly fragmented, global, interconnected, and governed by multiple regulators.[366]

Regtech solutions have promising applications to streamline compliance costs and processes.

[361] Kevin Petrasic, Benjamin Saul, James Greig, and Matthew Bornfreund, "Algorithms and Bias: What Lenders Need to Know," White & Case, January 20, 2017, https://www.whitecase.com/publications/insight/algorithms-and-bias-what-lenders-need-know.

[362] See *The USA Patriot Act*, Section 352.

[363] Fintech Circle Innovate CEO Nicole Anderson coined the term "regtech." See "The FinTech Influencers: FinTech, RegTech, and the Disruption of Banking's Services," Herrington Starr, May 26, 2015, http://www.harringtonstarr.com/fintech-influencers-fintech-regtech-disruption-bankings-services.

[364] Institute of International Finance, *Regtech in Financial Services: Technology Solutions for Compliance and Reporting*, March 2016, p. 4, https://www.iif.com/publication/research-note/regtech-financial-services-solutions-compliance-and-reporting.

[365] European Securities and Markets Authority, European Banking Authority, and European Insurance and Occupational Pensions Authority, *Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions*, JC 2016 86, Joint Committee of the European Supervisory Authorities, December 2016, file:///Users/mirenapariciobijuesca/Downloads/jc-2016-86_discussion_paper_big_data.pdf, 27.

[366] Caitlin Long, "*Why Financial Regulators Are Warming to Blockchains and Rightfully So*" in Alt-M Ideas for an Alternative Monetary Future, (April 2016), http://www.alt-m.org/2016/04/26/why-financial-regulators-are-warming-to-blockchains-and-rightfully-so/

Artificial intelligence systems and robotic processes automation have huge potential to complement big data analytics, such as for anti-money laundering and client identification, which are related to compiling and checking data on customers and transactions. A number of regtech providers are developing systems for using blockchain for digital identity purposes.

"Several countries are testing the development of a digital identity. . . When approved, it could be leveraged by banks to facilitate KYC processes."

An example of a new information source to conduct KYC and background checks are web crawlers, which can scan the Internet and deliver their data to big data infrastructures in real time.[367] In the future, machine learning could be promising to monitor suspicious transactions on a risk-based customer profile.

Regtech technologies, such as biometric validation for digital identity and KYC purposes—including facial, voice, fingerprint, and iris recognition—are evolving rapidly. Citigroup's 2017 *Digital Disruption Revisited*[368] report explores regtech as an opportunity for banks to explore the use of artificial intelligence and biometric identification for anti-money laundering and client identification, since "over the longer term, a nationwide [know your customer] utility could be beneficial to the whole society, and many regulators and governments are working towards this ideal."[369]

Customer due diligence infrastructure requires analyzing information from private and public sources in different languages and formats, which vary from country to country. Regtech providers can aggregate data worldwide. As an example, identity verification companies provide access to data collected in fifty countries from a variety of sources; data intelligence platforms collect information about financial crimes from media sources.

Regtech innovation can also help governments provide citizens with a digital identity.[370] As the US Department of Commerce's *Digital Identity Guidelines* define it:

> Digital Identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject. In other words, accessing a digital service may not mean that the physical representation of the underlying subject is known. Identity proofing establishes that a subject is actually who they claim to be. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity.[371]

Several countries are testing the development of a digital identity, such as the Monetary Authority of Singapore, which is developing a digital proof of identity tool on mobile phones. When approved, it could be leveraged by banks to facilitate KYC processes. Estonia[372] is another example of progress in this area. Estonians have a digital identity embedded in a SIM card, which they can use for digital signatures for every legal document and voting.[373]

Another successful example is Aadhaar, a digital identity program that has been introduced in India and is targeting one billion citizens on a voluntary basis, to be identified and authenticated by the use of biometrics (fingerprints and scan of the iris).[374] The Aadhaar digital identity project aims

[367] Institute of International Finance, Deploying Regtech Against Financial Crime, March 2017 p 17 ss. https://www.iif.com/system/files/32370132_aml_final_id.pdf

[368] "What FinTech VC Investments Tell Us about a Changing Industry," Citi GPS, January 23, 2017, https://www.privatebank.citibank.com/home/fresh-insight/citi-gps-digital-disruption-revisited.html.

[369] Martin Arnold, "Banks' AI Plans Threaten Thousands of Jobs," *Financial Times*, January 25, 2017, https://www.ft.com/content/3da058a0-e268-11e8-8405-9e5580d6e5fb.

[370] See the Draft Digital Identity Guidelines, provided by National Institute of Standards and Technology, DRAFT NIST Special Publication 800-63-3 *Digital Identity Guidelines*, US Department of Commerce, 2017, https://pages.nist.gov/800-63-3/sp800-63-3.html.

[371] Ibid.

[372] See "Fact," e-Estonia.com, https://e-estonia.com/facts/.

[373] Citigroup Global Perspectives and Solutions, *Digital Disruption – Revisited – What FinTech VC Investments Tell Us about a Changing Industry*, January 2017, https://ir.citi.com/rc3XP%2FtfuLrOmpDrBN2nNfJpkI7892Pd71h7%2BpDMbIosIS3u8kcgSiJoKWuI6p6RLpMUB0DYajQ%3D, 40.

[374] Reserve Bank of India, *Committee on Comprehensive Financial Services for Small Businesses and Low Income Households*, 2013, via World Bank, http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/282884-1339624653091/8703882-1339624678024/8703850-1368556147234/India-Financial-Inclusion-Report-RBI-CMTE-CFS070114EFL.pdf, 7-21. See also World Bank, Transforming Digital Identity in India, http://www.worldbank.org/en/news/video/2016/01/13/transforming-government-digital-identity-in-india

to avoid fraud with the creation of a centralized database including information on citizens deterred by any government agency. Digital identity can promote financial inclusion. Any potential welfare and healthcare benefits provided by the Indian government can be disbursed through a digital account associated with each citizen's mobile phone using this system.[375]

Digital identity uses are promising but also present the technical challenge of cybersecurity: "...because this process often involves the proofing of individuals over an open network, and always involves the authentication of individual subjects over an open network to access digital government services. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks."[376]

Blockchain, Distributed Ledger Technologies, and Smart Contracts

Financial supervisory agencies are welcoming blockchain as a transparent ledger that will help supervise securities trading and settlements due to the "practical impossibility of a single national regulator collecting sufficient quality data . . . to recreate a real-time ledger of the highly complex, global swaps trading portfolios of all market participants."[377] Digital Asset Holdings' December 2016 *Digital Asset Platform: Non-Technical White Paper* defines a distributed ledger technology (DLT) as "a record of transactions or other data which exists across multiple distinct entities in a network."[378] Its application for different uses is evolving rapidly, from transaction registries to other forms of data and encoded business logic. Central banks, exchanges, governments, and financial market participants are starting to use DLTs for several purposes, including issuing digital currencies and creating securities infrastructure with reduced operational risk, data integrity, and increased market transparency while protecting confidentiality.[379]

Smart contracts were defined by computer scientist Nick Szabo in 1996 as a "set of promises, specified in digital form, including protocols within which the parties perform on these promises."[380] The white paper prepared in December 2016 by the Smart Contracts Alliance, an initiative of the Chamber of Digital Commerce, explores in detail twelve use cases for businesses. Smart contracts are typically deployed on a blockchain, although they can be used on other platforms. Blockchain technology uses encryption messages, which are bundled together in a software-generated container (a block), relating to a particular smart contract. In permissioned (closed) blockchains, an administrator incorporates the encrypted messages into the secured data. The white paper points to promising potential applications of smart contracts for digital identities, company registrations, financial data or land title recordings, supply chains, insurance, mortgages, trade finance, and clinical trials, among other areas.[381]

Smart contract applications for digital identities (for individuals and companies) could represent a valid alternative for mitigating financial crime risk and streamlining compliance with KYC processes for financial firms. A digital identity for individuals and legal entities could potentially be issued by a regulatory agency that controls the identity's personal data and is able to securely disclose them to different counterparties (such as banks) in a blockchain, as needed.[382] An interesting and innovative public initiative by Delaware (the Delaware initiative), in partnership with a fintech company,

[375] World Bank, *Digital Identity Toolkit: A Guide for Stakeholders in Africa,* June 2014, http://documents.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf.

[376] National Institute of Standards and Technology, DRAFT NIST Special Publication 800-63-3 *Digital Identity Guidelines*, US Department of Commerce, 2017, https://pages.nist.gov/800-63-3/sp800-63-3.html.

[377] Commodity Futures Trading Commission Commissioner J. Christopher Giancarlo speech before the CATO Institute, "Cryptocurrency: The Policy Challenges of a Decentralized Revolution*,*" April 2016, US Commodity Futures Trading Commission, http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-14; see also Mary Jo White, "Opening Remarks at the SEC Fintech Forum" US Securities and Exchange Commission, November 2016, https://www.sec.gov/news/statement/white-opening-remarks-fintech-forum.html.

[378] Digital Asset Holdings, *The Digital Asset Platform,* December 2016, http://hub.digitalasset.com/hubfs/Documents/Digital%20Asset%20Platform%20-%20Non-technical%20White%20Paper.pdf?utm_campaign=whitepaper-non-tech&utm_medium=email&_hsenc=p2ANqtz-9kX1tI0v3HDSL4FBF2JCelw-TrrhFvbkqsrl_lqGfRwSbWk00bu1VqUmQqgK_SSKdlxDAtq05ciM8q-BsommkSxGP3EF-UgkJAhInC9DE4eQx89hl&_hsmi=38825746&utm_content=38825746&utm_source=hs_email&hsCtaTracking=fc1f9260-0c14-472a-967e-c9cb3095f953%7Cba8116ac-3c0b-43f3-a880-d60c4bc1d707, 4.

[379] Ibid., 27.

[380] See Nick Szabo, "Foreword" in *Smart Contracts: 12 Use Cases for Business & Beyond*, Chamber of Digital Commerce, December 2016, https://gallery.mailchimp.com/a87f67248663abe55ad9325d6/files/Smart_Contracts_12_Use_Cases_for_Business_Beyond.pdf?utm_source=Chamber+of+Digital+Commerce&utm_campaign=4123b7a006-EMAIL_CAMPAIGN_2016_12_06&utm_medium=email&utm_term=0_e6622a916a-4123b7a006-338085917

[381] *Smart Contracts: 12 Use Cases for Business & Beyond*, Chamber of Digital Commerce, December 2016, https://gallery.mailchimp.com/a87f67248663abe55ad9325d6/files/Smart_Contracts_12_Use_Cases_for_Business_Beyond.pdf?utm_source=Chamber+of+Digital+Commerce&utm_campaign=4123b7a006-EMAIL_CAMPAIGN_2016_12_06&utm_medium=email&utm_term=0_e6622a916a-4123b7a006-338085917.

[382] See also Ibid., 6-48.

A bitcoin ATM machine enables the user to convert cash to bitcoins via a QR code transfer to an application on their mobile device. *Photo credit:* Reuters/Mike Blake.

is the development of a new public repository to incorporate companies in 2017—corporations will have the choice of registering either via traditional stock certificates or on a blockchain. Registering companies through blockchain could facilitate performing due diligence, registering beneficial ownership during a corporate lifecycle, and, in the future, issuing digital securities.[383]

Stricter Bank Supervision in Emerging Nations

Money launderers do not respect borders. Financial Intelligence Units and law enforcement authorities have jurisdictional limitations and often lack resources. As a result, criminals can exploit jurisdictional gaps to circumvent AML national laws.

The Financial Stability Board has recently recommended stricter bank supervision and financial crime law enforcement in developing nations to halt the decline in correspondent banking ("de-risking"). The FSB statement recognizes that many emerging countries have adopted AML laws but do not enforce them or lack capacity to adequately supervise banks. As a consequence, banks in the US and other developed economies, particularly in Europe, as per Bank of International Settlements statistics on July 2016, have increasingly withdrawn from doing business in high-risk jurisdictions.[384]

As the Comptroller of the Currency stated before the Institute of International Bankers in 2016: "if U.S.-chartered financial institutions have a clear understanding of the risks associated with their

[383] Delaware Office of the Governor, "Governor Markell Launches Delaware Blockchain Initiative. Reflects State's Commitment to innovation and Embracing the New Economy," Press Release, May 2016, http://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html; see also Delaware Chancery Court Judge J. Travis Laster speech before the Council of Institutional Investors (Chicago), "The Block Chain Plunger: Using Technology to Clean Up Proxy Plumbing and Take Back the Vote," Council of Institutional Investors, September 2016, http://www.cii.org/files/09_29_16_laster_remarks.pdf.

[384] Binham, "Stricter Bank Supervision Needed in Developing Nations, Say Policymakers."

correspondent banking clients and the jurisdictions in which they are located, they may be more comfortable providing banking services, even those services that may have historically had higher risk."[385]

International Cooperation

Recent successful international anti-corruption cooperation examples among law enforcement authorities include Odebrecht, Braskem, and International Soccer. As the US Justice Department announced in 2016 referring to sharing information among law enforcement authorities under the Foreign Corrupt Practices Act Pilot Program: "an international approach is being taken to combat an international problem."[386]

In the US v. Odebrecht case, the US jurisdiction was attracted via the use of US bank accounts by Odebrecht and Braskem in Miami. Odebrecht, a Brazilian conglomerate, engaged in 2001 in a scheme paying bribes to officials in several countries including Brazil, Angola, Argentina, Colombia, the Dominican Republic, Ecuador, Guatemala, Mexico, Mozambique, Panama, Peru, and Venezuela. The Justice Department called "an elaborate, secret financial structure" to pay $778 million in bribes over fifteen years. In exchange, Odebrecht asked politicians on retainer to pass friendly tax legislation and contracts with state-owned oil companies such as Petrobras.[387]

Braskem, a Brazilian petrochemical company, also participated in the scheme and received several contracts with Petrobras. Both companies pleaded guilty for corrupt payments and profits, which amounted to approximately $3.8 billion. The final penalty[388] for Odebrecht was determined to be $2.6 billion in April 2017 (initially estimated at $4.5 billion but negotiated down since Odebrecht admitted it could not pay the fine). Brazil would receive 80 percent of the recovery, with the United States and Switzerland receiving 10 percent each. Braskem pleaded guilty to violating the Foreign Corrupt Practices Act and agreed to pay a criminal penalty of $632 million. Brazil would receive 70 percent of it, with the United States and Switzerland receiving 15 percent each.

International cooperation mechanisms among law enforcement authorities and Financial Intelligence Units and exchange of information should be prioritized and reinforced. Another successful example of international anti-money laundering cooperation between the US Treasury and foreign governments was the US Treasury's declaration in October 2015 of Banco Continental (Honduras) Group as "specially designated narcotics traffickers," which allows the freezing of assets in the United States due to money laundering.[389] The Honduran authorities cooperated in the investigation and liquidated the Honduran bank, which had been involved in money laundering activities for a decade.

The Egmont Group is composed of a number of FIUs that have been working together since their first meeting in Brussels in 1995, at the Egmont-Arenberg Palace.[390] The group provides a forum for FIUs that allows them to share information through memoranda of understanding meant to improve anti-money laundering programs. The exchange of financial intelligence can generate evidence in fighting financial crime and improve FIU expertise.[391]

At the European level, the European Commission's recent proposal of 5AMLD would enhance the FIUs' authority to access information from any covered entity in Europe across national borders by setting up automated centralized mechanisms in the form of (i) a central data registry of holders of banking and payment accounts or (ii) central data retrieval systems.[392] The interconnection of central registries would also increase transparency.[393] Moreover, the recent proposal to set up a strong independent European Public Prosecutor's Office with authority over all types of financial crimes affecting the EU

[385] Remarks by Thomas J. Curry, Comptroller of the Currency, March 7, 2016, https://www.occ.gov/news-issuances/speeches/2016/pub-speech-2016-25.pdf.

[386] US Department of Treasury, "Treasury Announces Key Regulations and Legislation to Counter Money Laundering and Corruption, Combat Tax Evasion," Press Release, May 5, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx.

[387] Acting Assistant Attorney General Kenneth A. Blanco, "Statement at the American Bar Association National Institute on White Collar Crime" (speech, Miami, FL, March 10, 2017), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-kenneth-blanco-speaks-american-bar-association-national.

[388] United States of America v. Odebrecht S.A., Plea Agreement, https://www.justice.gov/opa/press-release/file/919911/download

[389] Gustavo Palencia and David Alire Garcia, "Honduran Bank at Center of Money Laundering Case to Be Shut Down," Reuters, October 11, 2015, http://www.reuters.com/article/honduras-crime-banking-idUSL1N12B0I820151012.

[390] Egmont Group, *Principles for Information Exchange between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases,* June 2011.

[391] See Egmont Group, *100 Cases from the Egmont Group,* http://www.egmontgroup.org/library/cases.

[392] See 5AMLD approved by the EU Council, *Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849*.

[393] See proposed Measures 3 and 4 under the European Commission, "*Anti-Money Laundering and Counter Terrorist Financing: Stronger Rules to Respond to New Threats,* 2016, http://ec.europa.eu/justice/criminal/document/files/aml-factsheet_en.pdf, 2-4.

budget could be an important step in preventing financial crime.[394]

Independent Assessments for High-Risk Jurisdictions

Evaluating the money-laundering risk in several countries and jurisdictions requires looking at different sources. FATF identifies jurisdictions that have strategic AML deficiencies and works with them to address those deficiencies that pose a risk to the international financial system.[395] Countries that are often in the media for corruption, drug trafficking, and terrorism generally qualify as high-risk jurisdictions. Most AML laws require banks to conduct enhanced due diligence processes for customers doing business in high-risk countries. Banks, governments, and private firms use data analytics tools to pool data when evaluating country risk. Country risk analytics tools generally use algorithms to weigh and process data gathered from public and private sources. When choosing data analytic tools, it is important that the data are comprehensive, accurate, and frequently updated.

Countries in sanctions lists published by the United Nations, the United States, United Kingdom, and European Union need to be monitored by global banks to avoid regulatory fines. Country reports and evaluations published by international financial institutions, such as the International Monetary Fund and the World Bank, are also useful information sources to assess country risk. A frequent source of information for country risk analysis is the US Department of State's global annual report on money laundering and financial crime, which provides country evaluations based upon the contributions of numerous US government agencies and international sources.[396]

In 2010, FATF issued guidance concerning how it would identify certain high-risk countries by describing specific strategic AML deficiencies. The FATF conducts mutual evaluations (peer-to-peer reviews) on member countries' compliance with respect to its recommendations. In February 2013, FATF developed a methodology for AML country assessments.[397]

The IMF has endorsed the FATF 2012 recommendations and 2013 methodology. The IMF's financial integrity reviews apply to selected cases of Article IV consultations (surveillance programs), which are similar to annual audits the IMF holds with each member state, as well as its Financial Sector Assessment Program (FSAP). FSAPs are in-depth examinations of the financial sector, conducted by the IMF (jointly with the World Bank in the case of developing nations), and are associated with an Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) review. The IMF's 2012 Guidance Note sets out a number of criteria that guide staff in determining whether financial integrity issues should be included in the IMF's surveillance programs.[398] The Guidance Note refers to cases where money laundering, terrorism financing, and related crimes (such as corruption or tax crimes) are serious enough to threaten domestic stability, balance of payments stability, or the effective operation of the international monetary system.[399]

The IMF's corruption reviews could be adopted more broadly, as recognized by its managing director, based on good governance principles.[400] Ukraine is an example where the endemic corruption has prompted the IMF to work with the authorities to propose anti-corruption measures and agencies, change public procurement rules, dismantle a company, and reform the judicial system. These good governance measures agreed to by the authorities were part of the IMF's economic recovery plan for Ukraine.[401]

Increasing transparency requests from stakeholders and donors should make international financial institutions consider promoting financial integrity and good governance for financial assistance

[394] See "Anti-Money Laundering, European Public Prosecutor's Office, Digital Contracts, and Insolvency," Speech by Commissioner Jourová to the Legal Affairs Committee and EU Affairs Committee in the Bundestag, September 26, 2016, http://europa.eu/rapid/press-release_SPEECH-16-3189_en.htm.

[395] FATF, Public Statement, April 2017, http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-february-2017.html

[396] See US Department of State, *Volume II: Money Laundering and Financial Crimes*, 2016, http://www.state.gov/j/inl/rls/nrcrpt/2016/vol2/index.htm.

[397] FATF, *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems,* February 2013, http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.

[398] International Monetary Fund, *Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism,* February 2014, https://www.imf.org/external/np/pp/eng/2014/022014a.pdf, 15, Sections 25, 26 and 27.

[399] The IMF and the Fight Against Money Laundering and the Financing of Terrorism, May 2017, http://www.imf.org/external/np/exr/facts/aml.htm

[400] Remarks by Christine Lagarde, "The Power of Transparency to Increase Economic Resilience," at the Atlantic Council, February 8, 2017, https://www.youtube.com/watch?v=1ifk0OZMPvo.

[401] Ibid.

programs[402] based on: (i) the global reach of negative spillover effects of corruption, illicit financial flows, and trade-based money laundering; (ii) the increasingly global reach of virtual currency businesses (such as virtual currency exchanges and e-wallets), and the anonymity risk they represent as potential facilitators of illicit activities; and (iii) the recent recommendations by the Financial Stability Board for developing nations to strengthen bank supervision to halt de-risking in correspondent banking activities.

How To Help Government and Law Enforcement with Oversight Responsibilities

Expand the Use of Regtech, Automated Data Analytics, and Monitoring Systems

The Basel Committee report on sound management of risks related to money laundering and financing terrorism also recommends using automated risk analytics tools at a global level: "For most banks, especially those which are internationally active, effective monitoring is likely to necessitate the automation of the monitoring process. When a bank has the opinion that an IT [information technology] monitoring system is not necessary in its specific situation, it should document its decision and be able to demonstrate to its supervisor or external auditors that it has in place an effective alternative. . . . The IT monitoring system should enable a bank to determine its own criteria for additional monitoring, filing a suspicious transaction report (STR) or taking other steps in order to minimize the risk."[403]

The financial sector's obligation to report suspicious activities to a Financial Intelligence Unit exists in many countries. Technology is helping the financial sector analyze, filter, investigate, and process information on suspicious transactions. This should be complemented with regular training programs for employees. Most global banks have incorporated automated tools to help them comply with STRs and other regulatory or disclosure requirements. Whether they purchase software from vendors or develop their own monitoring programs, the important thing is to get the job done in capturing unusual client behavior patterns. US and EU financial crime enforcement authorities expect to test the technology during inspection visits to determine whether the system appropriately detects suspicious transactions. Given technological advances and the decreased cost of available systems, it would be difficult today for any US bank to claim that it is reasonable to rely on a largely manual system to identify and report suspicious transactions to authorities.[404]

> **"Technology is helping the financial sector analyze, filter, investigate, and process information on suspicious transactions."**

Multi-stakeholder Processes

Other countries should consider following the UK's lead in creating task force groups and opening channels of communication with the financial sector.[405] Such task force groups leverage intelligence that banks may have when conducting global business, beyond formal STRs reporting. Channels for direct dialogue between the financial sector and governmental agencies can prove mutually beneficial.

Public-private partnership initiatives (PPPIs) are often led by international financial institutions in partnership with international banks, government agencies, and the private sector to boost investments in the energy, water, infrastructure, and transport sectors. As the lead adviser, international financial institutions work with governments on legal and regulatory requirements to build technical capacity. International financial institutions should consider including financial integrity safeguards, similar to environmental and social safeguards, in their design of the PPPI strategies. These are key to fostering transparent bidding processes and good governance and to avoiding corruption. Implementing these safeguards would also have the benefit of raising financial integrity standards for local partners.

[402] AML/CFT measures have been incorporated into conditionality under fund-supported programs in Afghanistan, Cyprus, Greece, Kyrgyzstan, São Tomé and Príncipe, and Uganda. See International Monetary Fund, *Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism,* February 2014, https://www.imf.org/external/np/pp/eng/2014/022014a.pdf, 17.

[403] Basel Committee on Banking Supervision, "*Sound management of risks related to money laundering and financing of terrorism,*" (Basel, 2016), 6-16.

[404] US Department of the Treasury Financial Crimes Enforcement Network, in re: "*Eurobank, San Juan, Puerto Rico*," (No. 2010-2), https://www.fincen.gov/sites/default/files/enforcement_action/AssessmentEurobank.pdf, 4; See also Financial Industry Regulatory Authority, *Anti-Money Laundering*, Special NASD Notice to Members 02-21.

[405] Jonathan Pickworth and Jonah Anderson, "New UK AML Action Plan – The Increased Role of the Private Sector," White & Case, April 28, 2016, http://www.whitecase.com/publications/alert/new-uk-aml-action-plan-increased-role-private-sector.

Voluntary Standards

The Wolfsberg Group is an example of how collective action from global banks can help promote strong international AML standards. Although the group has been criticized for being too formalistic and relying too much on information based on standard questionnaires, it is also recognized that these questionnaires have simplified the due diligence process for correspondent banking through data repositories. In addition to formal AML policies, the group should consider analyzing the efficiency of the automated controls currently in place to detect and monitor suspicious transactions and clients.

FATF recommendations have not been fully implemented in many countries and global banks face challenges operating in countries with weak financial crime regulations or enforcement. The Financial Stability Board has called on developing nations to adopt stricter banking supervision rules to halt the decline in correspondent banking relationships (de-risking).[406] Global correspondent banks can have a positive influence raising local standards to avoid de-risking, and creating incentives for local banks to voluntarily adopt higher AML standards, even if not required by local AML laws. Global asset managers and large pension funds can play a role in raising the corporate governance standards of the companies they invest in at a global level.

Recommendations

The following proposals could help underpin financial integrity if adopted at a global level:

- The Financial Stability Board, FATF, and regulators should work together to ensure that transparency exemptions for risk management and security purposes are addressed in privacy and other relevant laws to enable information-sharing regimes.
- The FSB should promote global regulatory coordination for the improvement of data formats and standardization of financial definitions for risk data aggregation.
- The FSB should develop international standards and best practices addressing cybersecurity.
- The FATF should provide clear definitions of key regulatory concepts and guidelines, such as Know Your Customer regulations or digital client onboarding due diligence.
- Financial regulators should promote the use of data analytics and monitoring tools by banks and their gatekeepers and fintech companies.
- Banks and supervisors should review rules that may hinder regtech experimentation.
- Emerging countries should reinforce financial supervision and explore technology innovation such as the issuance of digital identities to promote financial inclusion.
- International financial institutions should expand their role in promoting good governance programs and the adoption of FATF recommendations.
- Financial Intelligence Units should reinforce international cooperation and set up public-private task force groups to exchange informal intelligence.

Conclusion

Data analytics tools used by the public and private sectors to fight financial crime need high-quality and accessible data at a global level. Data protection or localization rules create obstacles to accessing data and sharing information across financial groups and lead to "silos" of information, against the Basel Committee's principles for effective risk data aggregation and reporting.[407]

As a result, for automated tools to effectively mitigate financial crime risks, privacy laws should include exemptions for data sharing based on transparency and security purposes. For instance, many jurisdictions, including the European Union, which has implemented FATF recommendations, require consent for processing personal data. Such privacy laws pose potential risks to accessibility and data quality, which are necessary to fight financial crime. The Financial Stability Board, FATF, and regulatory authorities should engage in international dialogue to favor certain risk-based exemptions for data sharing, permitting the processing and disclosure of personal data without a data subject's consent, to prevent fraud and corruption or for money laundering risk control. The Financial Stability Board should also intensify efforts for global regulatory coordination to improve standardization of data formats on financial concepts and definitions. A lack of data harmonization or insufficient detail of definition makes it hard to aggregate risk data across financial groups and jurisdictions on an automated basis.[408]

[406] See Binham, "Stricter Bank Supervision Needed in Developing Nations, Say Policymakers."

[407] Basel Committee on Banking Supervision, *Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, February 2016, http://www.bis.org/bcbs/publ/d353.pdf.

[408] Institute of International Finance, Regtech in Financial Services: Technology Solutions for Compliance and Reporting, March 2016, p. 4, https://www.iif.com/publication/research-note/regtech-financial-services-solutions-compliance-and-reporting

The FATF 2012 recommendations have not been enforced, or not fully enforced, in many countries. Such regulatory asymmetry creates gaps, which favor the circumvention of financial crime laws by moving the activities to jurisdictions, to the digital economy, or to unregulated sectors. To mitigate such risks, banks and other relevant players need to effectively use data analytics tools to monitor clients and transactions, and share intelligence with FIUs. Gatekeepers and new digital finance businesses (such as virtual currencies exchanges, money services businesses, and online lending platforms), should use automated data analytics tools, have effective AML frameworks, and report suspicious transactions, even on a voluntary basis. Emerging countries should explore regtech solutions such as digital identity to promote financial inclusion. They should also focus on stricter supervision of banks to avoid "de-risking," according to FSB. International financial institutions' role should be more prevalent in promoting good governance and financial integrity, consistent with FATF 2012 and Basel Committee recommendations. Financial Intelligence Units and law enforcement authorities should reinforce cooperation and exchange of information mechanisms at a global level, including public-private partnerships and task force groups.

Technological innovation, such as regtech and smart contracts, has the potential to effectively help banks streamline regulatory compliance processes and facilitate effective supervision by authorities. As an example, the global AML/CTF framework lacks universal definitions of key concepts, such as Know Your Customer or client due diligence requirements. National identification documents also vary from country to country. Placing KYC utilities on a distributed ledger could allow banks to share sensitive consumer data across several entities, facilitating KYC and supervision, without compromising nonpublic personal data (although it would not solve all the issues concerning data sharing). To mitigate the risk of experimenting with new technologies, regulators should set up an open dialogue with banks and start-ups to promote a "safe" environment and experimentation, where both supervisors and firms can work together to analyze how regulations can unintentionally impact automation and innovation, such as through requiring in-person identification instead of allowing digital identity verification methods.[409]

Fintech and regtech technologies that monitor customer activities may also increase cybersecurity and privacy risks.[410] Anytime an organization collects customer data, it must ensure that it preserves data from cyberattacks.[411] Regulators should change their supervisory focus as digitization changes the types of risk in the financial sector, shifting to cybersecurity risk. Ultimately, regulators need to set up international standards addressing legitimate privacy and cybersecurity concerns, while at the same time ensuring transparency and financial integrity, through dialogue with the private sector and the creation of new mechanisms to promote coordination among relevant agencies internationally to fight financial crime, protect data privacy, and uphold information security.

[409] Institute of International Finance, Deploying Regtech against Financial Crime, March 2017, https://www.iif.com/system/files/32370132_aml_final_id.pdf, 27.

[410] Citi Global Perspectives and Solutions, *E-Privacy and Data Protection: Who Watches the Watchers? How Regulation Could Alter the Path of Innovation,* March 2017, https://ir.citi.com/I%2FDe1TjhFWX1NpgDsXKJmsACj6DaypITsS7sNZ8DtTZvNvVHwHlNTmLogXdvmMMu727lshzkyVo%3D.

[411] Kevin Petrasic, Benjamin Saul, and Helen Lee, "Regtech Rising: Automating Regulation for Financial Institutions," White & Case, September 16, 2016, https://www.whitecase.com/publications/insight/regtech-rising-automating-regulation-financial-institutions.