International
Comparative
Legal Guides

Practical cross-border insights into anti-money laundering law

Anti-Money Laundering 2022

Fifth Edition

Contributing Editors:
Stephanie L. Brooker & Joel M. Cohen
Gibson, Dunn & Crutcher LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Impacts of COVID-19 and the Increasing Use of Technology for Financial Institutions


Stella M. Mendes


Greg Moscow

FTI Consulting

Introduction

On December 3, 2018, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network (FinCEN), National Credit Union Administration, and Office of the Comptroller of the Currency (OCC) issued a joint statement encouraging banks to implement innovative approaches to meet their Bank Secrecy Act (BSA)/anti-money laundering (AML) obligations. When discussing artificial intelligence (AI) and digital identity technologies, the statement said, "[t]hese innovations and technologies can strengthen BSA/AML compliance approaches and enhance transaction monitoring systems".[1] The regulators also noted that there would be no penalty if the approaches did not work or found issues that the bank's current system did not detect.[2] In May 2019, FinCEN created the Innovation Hours Program to promote responsible AML innovation. The Program allowed FinCEN to get a better understanding of new technologies. FinCEN staff learned about several key themes, including AI and machine learning (ML).[3]

Issues Raised During the First Year of COVID-19

According to the United Nations Office on Drugs and Crime, 2–5% of global GDP is laundered each year.[4] COVID-19 altered the methods of money laundering as well as how banks look to prevent it. The Financial Action Task Force (FATF), in their May 2020 report "COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses", laid out the money-laundering vulnerabilities that banks faced during the height of the pandemic, including:

- criminals bypassing customer due diligence (CDD) measures;
- increased misuse of online financial services and virtual assets;
- exploiting economic stimulus measures;
- increased use of unregulated financial sector;
- misuse and misappropriation of financial aid (corruption and consequent money-laundering risk); and
- criminals exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries.[5]

In December 2020, FATF issued an updated report and noted an increase in cyber-related scams "in particular email and SMS phishing schemes".[6] Additionally, FinCEN also issued advisories related to ransomware and cybercrime, including cyber-enabled financial crime, to alert covered institutions to predominant trends, typologies and potential indicators.[7] FinCEN also advised institutions that criminals are increasingly exploiting the pandemic through various tactics such as business email compromise, phishing scams, remote applications and other fraudulent schemes, especially against financial and healthcare systems.[8]

As the typologies of money laundering shift, banks need to ensure they have the flexibility to capture the new AML risk. The old rule-based approach to transaction monitoring coupled with CDD requirements helped banks establish their compliance programmes to be in accordance with best practices and industry regulations.[9] However, in order to maintain a well-functioning compliance programme, banks must adapt to the new AML risks. Financial institutions (FIs) and fintechs must also realise the importance of consumers' increasing appetite and trust for a digital-first approach to their finances. Customers are looking for security in their transactions and convenience; to achieve this, FIs will need to continue enhancing their efforts and alignment with market trends.

AML Compliance

Banks have responded to new methods of money laundering in a number of ways, including to update their rules and use AI/ML to improve what has become a check-the-box approach. Decision-making based on "defensive box-ticking approaches to risk, rather than applying a genuinely risk-based approach" is not helping banks to understand their risks.[10]

In 2019, LexisNexis looked at the true cost of AML compliance and found that U.S. financial services firms spend $26.4 billion on AML compliance a year.[11] The LexisNexis survey noted that "[s]maller firms are more challenged with AML compliance", and that "they tend to leverage compliance technologies less".[12] The survey asked FIs about their current use of new technology and services for AML compliance, and found that 25% of respondents said they used AI and ML.[13] At this point, technology cannot serve as a substitute for due diligence, and Know Your Customer (KYC): Paycheck Protection Programs loans processed by fintech firms were more likely to be obtained fraudulently.[14] In "The impact of Covid on machine learning and data science in UK banking", 50% of UK banks surveyed indicated that they expected an increase in the importance of ML for future operations.[15]

As banks look for ways to maintain or enhance their AML programmes while saving money, AI and ML offer solutions. Some FIs have already begun integrating AI/ML into their compliance programmes; but, according to a 2021 SAS study, 33% of FIs accelerated the integration process once COVID-19 hit.[16] Additionally, 57% of respondents said their institutions have either deployed AI/ML into their AML compliance process or are planning a pilot programme to do so by February 2023.[17]

For FIs to prepare for the upcoming regulations and increased enforcement, a strong compliance programme for AML, BSA and sanctions is the best place to start and build upon going forward. Every institution should ensure that its policies, procedures and risk assessments address new regulations, and that its system of internal controls reflects recent changes. Institutions should also test these to determine whether their internal controls can effectively detect and identify possible breaches of policies and procedures.

As these regulators continue to add more expectations for AML compliance programmes, banks face tremendous pressure to keep up. Many processes are carried out manually and are time-consuming: KYC compliance; fraud prevention; and AML are some examples. With AI/ML, there is an opportunity to streamline the manual tasks that happen behind the scenes. AI/ML can dramatically alter the banking landscape, giving rise to a new era of technological progress.

As AI/ML become more prevalent in AML compliance programmes, banks will need to demonstrate that they understand the technology they are using. It is easy for banks to explain their rules-based approach to combatting money laundering. The OCC views AI/ML as a new model that is subject to the Supervisory Guidance on Model Risk Management (SR 11-7).[18] Banks that use AI/ML models must understand, validate and challenge the results they receive, and as banks transition to using more AI/ML models, it is crucial for them to continue to follow these guidelines. As such models become more complex, there is a concern that they will become "black-box" models with incomprehensible behaviour.[19] FIs must ensure they understand and validate the results of the outputs of AI/ML. An additional concern for FIs is whether the initial data set has an implicit bias; in order to ensure that the data going into AI/ML is accurate, FIs must, at least on a yearly basis, go through a validation process.[20]

In 2022 and beyond, banks will continue to explore and implement innovative AI/ML solutions, increasing their ability to maintain risk-based compliance programmes. The data provided by AI/ML will enable FIs to better understand their inherent risk, their controls and their residual risk. The ability to correctly allocate resources will help banks to improve productivity and cut costs. Additionally, as the digitisation of customer identity and KYC processes continues, more people will have access to the banking system.[21]

With technology including AI/ML progressing rapidly in this space, we will see them become a standard tool in many processes, including data analysis. We are already seeing this in the fintech space, where companies have shown that technology can help provide customers with a better experience. Banks should consider digitising their KYC processes sooner rather than later to stay in competition with fintech startups, whose businesses will have experienced growth and evolution from the get-go; they will also come without legacy systems that many banks have had to grow around. Since 2019, there has been an increase in the number of fintechs and banks partnering with one another: in 2019, fintechs averaged 1.3 partnerships per institution, a number that grew to 2.5 in 2021.[22]

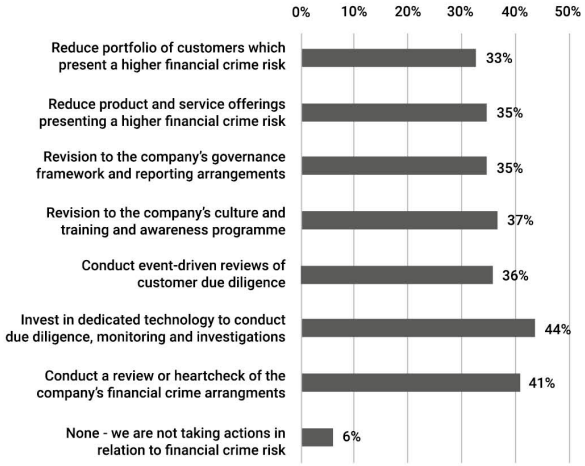
Regulators have encouraged banks to implement innovative approaches to meet their compliance obligations and to better protect the financial system from illicit financial activity.[23] Banks are continuing to look for more intelligent, data-driven processing to combat financial crime. AI/ML can assist FIs in detecting fraud and ensuring regulatory compliance by reducing the risk of non-compliance with KYC requirements.[24]

With the addition of technologies such as AI/ML, FIs should review legacy processes, including policies and procedures within the bank, and determine if there are ways to digitise the processes. Additionally, FIs should reduce staff intervention – where manual customer reviews occur on an exception basis only, freeing up staff to concentrate on higher risk functions, while still meeting KYC compliance requirements and improving interaction with clients. AI and ML are at a tipping point; banks need to be able to adopt these technologies in order to compete and stay compliant. AI and ML have changed the banking landscape permanently, impacting everything from customer experience to regulatory compliance; and in the years to come, we will see even more dramatic advances in this space.[25]

Banks that have a solid understanding of their customers and create a strategy around AI/ML today will be well positioned to take advantage of these opportunities as they arise in the years to come. In a recent press release, Kieran Beer's comments to SAS stated: "As regulators across the world increasingly judge FIs' compliance efforts based on the effectiveness of the intelligence they provide to law enforcement, it's no surprise 66% of respondents believe regulators want their institutions to leverage AI and machine learning."[26]

According to FTI Consulting's Resilience Barometer, "52% of North American financial services firms strongly agree that a growing number of criminals are exploiting the financial system. Yet just 26% are planning to reduce their portfolio of customers which present a higher financial crime risk, compared to 41% and 36%, respectively, for their counterparts in APAC and EMEA. One interpretation is that North American firms are more confident than their global counterparts in their screening arrangements and financial crime control frameworks – and that previous de-risking exercises have already 'done the job'".[27] As technology advances, we will continue to see developments in fighting financial crime and mitigating sanctions risk; and as criminals evolve, so must businesses. According to the FTI Resilience Barometer, 44% of large G20 companies surveyed have already invested – or are planning to invest – in dedicated technology to conduct due diligence, monitoring and support investigations in 2022 (see Fig. 1). There are some investigative software platforms that allow companies to conduct detailed transactional analyses, including identification and clustering of high-risk wallet address and tracing of virtual currency transactions. FIs and fintechs can use these technologies to better understand the risk cryptocurrency transactions represent.

Fig. 1: Current and future plans in relation to financial crime risk

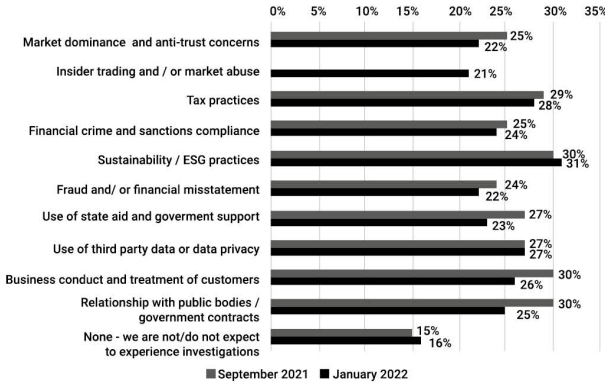


Cryptocurrency

Both the use of and investments in cryptocurrencies have significantly increased since the onset of COVID-19. On March 1, 2020, there were 7,119 Bitcoin ATMs globally. By March 1, 2022, there were 36,023.[28] During the ongoing COVID-19 pandemic, people have used crypto assets for loans and other traditional banking transactions. Seeing the increase in use of cryptocurrencies, regulators have strengthened their focus in this area and, as the pandemic continues, we will see further developments; for example, President Biden's Executive Order on strategy and development of digital assets and crypto.[29] The Order outlines the implications of digital assets in consumer protection, financial stability, national security, illicit financing and climate risk.

FIs must comply with AML rules, KYC regulations and appropriate sanctions. Now more than ever, the digital asset industry must articulate its value and provide responsible regulatory compliance standards, as cryptocurrency and blockchain are no longer prospects of the future. More than 80% of G20 organisations are now considering implementing these technologies, and 66% are currently piloting or exploring how blockchain and digital assets can play a role in their business offering (see Fig. 2). The appetite for adoption is highest in China (85%) and India (83%).[30]

Fig. 2: Areas companies face or anticipate regulatory or government investigations



With the continuous shift in the operating landscape, such as a more hybrid workforce, threats have evolved and organisations face a range of cybersecurity risks, including new phishing or social engineering techniques, the use of personal devices while working remotely and emerging technologies. Among Chief Information Security Officers (CISOs), 43% believe new and emerging technologies, such as blockchain and AI, are the top risks – contradictorily, 66% of respondents are piloting or exploring how blockchain and digital assets can play a role in their business offering, suggesting that they see benefits in adopting new technology despite the risks.[31]

A fact sheet recently issued by FinCEN encourages information sharing among covered institutions, under a safe harbour provision of the BSA that offers protections from civil liability in order to better identify and report potential money laundering or terrorist financing.[32] There is a higher burden on FIs, as they are required to detect suspicious activity that results from cybercrime. FIs are also required to report potential wrongdoing in their everyday transactions with suspicious activity reports (SARs). This leads FIs to strengthen their mechanisms that review and monitor systems, and continue to evaluate the transactions that happen within them. This also identifies a greater need to have workers with the skillset to be able to identify illegal activities and report them immediately.

In September 2021, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) issued an updated advisory on potential sanctions risks for facilitating ransomware payments, designed to disrupt criminal networks and virtual currency exchanges. Regulators expect FIs to have robust processes in place to assess and identify sanctions risks, particularly associated with clients, and take appropriate steps to mitigate those risks. FIs have an increasing number of issues to consider when performing KYC due diligence and transaction sanctions monitoring. The sanctions due diligence that a FI or regulated entity conducts at the outset of a client relationship or transaction, and periodically thereafter, is critical to managing sanctions risk.[33]

More than ever, FIs must be able to identify emerging sanctions risks and respond with appropriate measures. Fintech is an emerging area in which FIs must understand their legal obligations and risk exposure. Digital currencies, particularly cryptocurrency, present heightened sanctions risks. Institutions that have not created cryptocurrency-related offerings for their customers (e.g., trade or custody of cryptocurrency, investment in cryptocurrency exchanges) face potential sanctions risks associated with cryptocurrency, since it can be used to evade sanctions. The ability to identify potential cryptocurrency-related transactions, including those related to sanctions evasion, is critical.

While companies continued to focus on maintaining business and solvency during the earlier period of the pandemic, many corporations de-prioritised substantial compliance and information governance programmes. We also see that the incidence and impact of data breaches do not appear to be lessening, and there is a critical need for reinvestment in and renewed focus on information governance and privacy programmes. Overall, many organisations expect their data risk to increase in the coming year.

Case Studies

FTI Consulting was engaged as the independent consultant on behalf of the regulators to conduct a comprehensive review of the New York branch of a global European bank's current BSA/AML and sanctions compliance programme, as well as a transaction review and testing. The review included an assessment of the bank's policies, procedures and processes as well as an evaluation of the controls in place.

FTI reviewed all aspects of the programme, including areas such as training, staffing, management oversight, independent testing and "rule book" testing. FTI also tested and verified the remediation of deficiencies in the bank's BSA/AML compliance programme that were identified by the compliance review, and audited the results of a transaction lookback the bank was to complete.

The work focused on the following components of the bank's BSA/AML compliance programme: suspicious activity monitoring and reporting; CDD; internal audit; and corporate governance and management oversight. FTI's role in analysing and testing the bank's remediation efforts required two years of close coordination and communication with the bank and the regulator, during which time the bank made major structural changes to its compliance programme, business model, core operations and strategic priorities.

Conclusion

FIs and companies need to be aware of the radical changes brought on by the COVID-19 pandemic, not just from emerging COVID variants, but from new technologies and how they can best be implemented into everyday transactions. Whether businesses are trying to enhance their practices, engage more

effectively with their customers or effectively enhance their operations, they will need to explore and maintain best practices. Businesses will take varied approaches to leverage the opportunities presented by the pandemic and new technologies, but when it comes to compliance, they must be aligned with the stance of regulators and how new legislation will affect each aspect of their business.

With the rise of digital assets and virtual currencies, money laundering and financial crimes have become an even more imminent danger to the stability of FIs. Regulatory agencies worldwide are encouraging FIs to implement AI/ML tools to help combat these crimes. In a rapidly evolving industry, each FI should continue to assess its readiness for increased oversight and apply new technologies and techniques to achieve the highest standards of compliance.

Endnotes

1. https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29.pdf.
2. *Ibid.*
3. https://www.fincen.gov/news/news-releases/fincens-innovation-hours-marks-one-year-milestone.
4. https://www.unodc.org/unodc/en/money-laundering/overview.html.
5. https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf.
6. https://www.fatf-gafi.org/media/fatf/documents/Update-COVID-19-Related-Money-Laundering-and-Terrorist-Financing-Risks.pdf.
7. See FinCEN, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, October 1, 2020; FinCEN, Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic, July 30, 2020.
8. See FinCEN, Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic, July 30, 2020.
9. https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29.pdf.
10. https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf, p. 11.
11. LewisNexis® Risk Solutions 2019 True Cost of AML Compliance Study, p. 4.
12. *Id.*, p. 8.
13. *Id.*, p. 11.
14. https://bankingjournal.aba.com/2022/02/a-moving-target-pandemic-impacts-on-anti-money-laundering-compliance/.
15. https://www.bankofengland.co.uk/quarterly-bulletin/2020/2020-q4/the-impact-of-covid-on-machine-learning-and-data-science-in-uk-banking#footnote-1.
16. https://www.sas.com/en_hk/news/press-releases/2021/august/global-aml-study-pandemic-spurs-ai-adoption.html.
17. *Ibid.*
18. https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf.
19. *Ibid.*
20. https://engineering.dynatrace.com/blog/understanding-black-box-ml-models-with-explainable-ai/.
21. https://id4d.worldbank.org/global-dataset.
22. https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29.pdf.
23. https://www.forbes.com/sites/louiscolumbus/2019/07/09/top-9-ways-artificial-intelligence-prevents-fraud/?sh=6191d48214b4.
24. https://www.forbes.com/sites/ronshevlin/2022/01/19/bank-fintech-partnerships-are-under-performing-whats-going-wrong/?sh=3a5e851559a2.
25. https://www.infosys.com/aimaturity.html.
26. https://www.sas.com/en_hk/news/press-releases/2021/august/global-aml-study-pandemic-spurs-ai-adoption.html.
27. https://live.fticonsulting.com/ResilienceBarometer2022.
28. https://coinatmradar.com/charts/growth/, accessed April 21.
29. https://www.nytimes.com/2022/03/09/us/politics/crypto-regulation-biden.html.
30. https://ftiresiliencebarometer.com/the-resilience-agenda.
31. *Ibid.*
32. See USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 314(b) (2001); 31 CFR § 1010.540; FinCEN, FinCEN Director Emphasizes Importance of Information Sharing Among Financial Institutions, December 10, 2020.
33. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

Stella M. Mendes, CAMS, is the Leader of the Financial Services practice at FTI Consulting, focusing on financial institutions, bank governance and regulations. She has more than 25 years of diverse banking industry experience and is based in New York.
Ms. Mendes leads BSA/AML reviews for banks, money service businesses, credit unions and other financial service providers. She has established and enhanced BSA/AML/OFAC policies, procedures and processes to ensure compliance with regulations. She has also led multiple compliance "look-back" reviews. She consults with clients on BSA and AML best practices, performs reviews and enhancements of BSA/AML/OFAC Risk Assessments and conducts AML investigations as part of governmental investigations. Ms. Mendes provides advisory services on regulatory responses, AML training to banks and other financial services firms and gives webinars on regulatory compliance best practices. She also assists clients with other regulatory compliance matters.

FTI Consulting
1166 Avenue of the Americas
15th Floor
New York, NY 10036
United States

Tel: +1 212 841 9363
Email: stella.mendes@fticonsulting.com
URL: www.fticonsulting.com

Greg Moscow is a Director in the Financial Services group at FTI Consulting and is based in New York City. His expertise includes knowledge of BSA, AML, Risk Assessments and OFAC. Since joining FTI Consulting, Mr. Moscow has worked on proactive and reactive matters for financial institutions. He has reviewed the remediation of an offshore trust company, OFAC compliance for a global FI and has reviewed and improved FI's risk management policies, including building a new risk management framework and reviewing model risk management policies. Mr. Moscow is CAMS certified and has a risk assessment certificate.

FTI Consulting
1166 Avenue of the Americas
15th Floor
New York, NY 10036
United States

Tel: +1 212 651 7131
Email: greg.moscow@fticonsulting.com
URL: www.fticonsulting.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group