Bloomberg Law

Professional Perspective

Global Anti-Money Laundering: Investigations and Compliance Trends in the Fintech Era

Amanda Raad, Ryan Rohlfsen, Matthew Burn, Patrick J. Reinikainen, and Ethan Thomas, Ropes & Gray

Global Anti-Money Laundering: Investigations and Compliance Trends in the Fintech Era

Contributed by Amanda Raad, Ryan Rohlfsen, Matthew Burn, Patrick J. Reinikainen, and Ethan Thomas, Ropes & Gray

A number of recent scandals involving alleged failures in anti-money laundering compliance have resulted in high profile investigations, placing some of the world's most prominent financial institutions in the spotlight for ignoring red flags for criminal money laundering and failing to implement adequate compliance controls. At the same time as rules governing anti-money laundering compliance are rapidly changing, forms of financial technology continue to evolve.

Blockchain, cryptocurrency, and AI have come squarely to the forefront of how institutions must identify and respond to risks associated with complex transactions. Companies seeking to ensure compliance with AML and Know Your Customer regulations should therefore continue to assess developing technology and the scope of investigations to design and implement effective AML compliance policies and procedures.

Key Developments in Global Investigations

In 2018, several U.S. regulators emphasized enforcement as a priority, continuing to aggressively pursue financial institutions for alleged failures and violations related to AML. Financial institutions faced scrutiny for ignoring red flags associated with potential money laundering schemes and for failing to implement sufficient internal controls to detect and respond to potential money laundering.

Many of these investigations arose following the wide-scale "Panama Papers" leak. Increased coordination between U.S. authorities—including the U.S. Department of Justice, the U.S. Securities Exchange Commission, and the U.S. Treasury Department's Financial Crimes Enforcement Network—and counterparts from other jurisdictions, including the U.K.'s Financial Conduct Authority, has increased the focus on potential AML violations.

Since 2008, there has been a growing regulatory and enforcement focus on AML compliance. According to a 2018 white paper, regulators in the U.S. and Europe alone imposed approximately $20 billion in fines, with year-on-year fines continuing to grow, particularly with respect to individual penalties. The U.S. leads in issuing fines globally, with the average fine nearing $200 million based on the top 11 regulators.

According to one report, surveyed data suggests that the aggregate amount of non-concurrent fines imposed by the Department of Treasury's Financial Crimes Enforcement Network and federal banking regulators alone surpassed $307 million in 2018, rising significantly from 2016 when U.S. enforcement and regulatory authorities imposed only $24 million. In 2018, the Office of the Comptroller of the Currency assessed the largest such penalty of $100 million.

The DOJ and SEC also had an active year, pursuing a number of high-profile cases that resulted in significant penalties stemming from AML compliance failures, with penalties in one case totaling $528 million. Such cases were frequently pursued in parallel, resulting in often-staggering aggregate penalties and even significant individual liability for culpable executives and compliance officers. In addition, regulators at the state level continued to aggressively pursue AML violations and failures, with the New York State Department of Financial Services leading the pack in imposing penalties.

Although the U.S. has taken the lead in aggressive enforcement, last year a number of significant penalties were also imposed within Europe against various institutions, revealing that European authorities also demand robust compliance frameworks. Mark Steward, the FCA's Director of Enforcement and Market Oversight, recently stated that the agency was prepared to criminally prosecute firms regulated by the agency for AML failings. He said "it is time that we gave effect to the full intention of the Money-Laundering Regulations which provides for criminal prosecutions. In making poor AML systems and controls potentially a criminal offence, the MLRs are signaling that, in egregious circumstances, MLR failures let down the whole community."

As of April 9, 2019, the FCA had imposed £272 million in fines, of which a large proportion related to failures in AML compliance with money laundering regulations. Moreover, for the year-end 2017/2018, the FCA opened more cases than in any year in its history. The FCA's business plan for 2019 also makes clear the growing need to tackle money laundering within the U.K.'s financial sector; this will be one of the FCA's key priorities in the year ahead.

This point was echoed by Lisa Osofsky, the new Director of the U.K.'s Serious Fraud Office, shortly after her appointment in Sept. 2018. As part of its approach, the FCA intends to further deploy the use of machine learning techniques as well as further data sharing among enforcement agencies. U.K. and U.S. regulators have focused on individual liability, placing an emphasis on identifying employees behind AML violations and failures.

As a reflection of this prioritization, the FCA has implemented the Senior Manager Certification Regime, which appears to be part of a process of highlighting the importance of individual accountability for employees performing senior management functions within banks. Among other requirements, this process necessitates a clear delineation of roles and responsibilities, as well as regulatory approval for "senior managers" to carry out their functions.

Although Brexit may entail uncertainty, these recent developments signal that enforcement in 2019 will continue to focus on widespread AML compliance failures and rooting out individual wrongdoing, with high penalties continuing to be part of the enforcement strategy in both the U.S. and Europe.

Regulatory and Legislative Developments in Anti-Money Laundering

Adding to the steady stream of investigations and penalties, the regulatory landscape also continues to evolve, further complicating AML compliance efforts. In addition to state-level rules and regulations, AML compliance has traditionally been governed by regulations under the Bank Secrecy Act and USA Patriot Act, among others. However, new developments continue to bolster this legal framework by adding to the already substantial requirements imposed on covered financial institutions. For example, FinCEN promulgated the Customer Due Diligence rule in May 2018. 31 C.F.R. §1010.230. The CDD rule, developed as a means to promote transparency following the Panama Papers scandal, modified the BSA regulations such that "financial institutions will have to identify and verify the identity of any individual who owns 25 percent or more of a legal entity, and an individual who controls the legal entity."

Under the rule, financial institutions must verify the identity of all customers, as well as the beneficial owners of corporate customers. The institutions are also required to "understand the nature and purpose of customer relationships to develop customer risk profiles" and conduct ongoing suspicious transaction monitoring.

Even in the absence of formal federal regulation, U.S. agencies and states continue to add to businesses' AML/KYC obligations, particularly as new sectors (such as virtual currency) continue to grow. A recent example of a state regulation is NYDFS 504 from New York. This rule requires certain businesses to implement, assess, and document their AML procedures, which must include risk-based transaction monitoring and filtering programs.

In the EU, the pace of regulatory development in the AML space has been rapid. Member states had only just implemented 4AMLD in summer 2017 when the fifth Anti-Money Laundering Directive came into force on July 9, 2018. EU member states have until Jan. 10, 2020, to give effect to its provisions in their national laws. Notably, 5AMLD marks the first attempt by the EU to regulate virtual currency. It extends the AML requirements set out in 4AMLD, which had applied inter alia to traditional financial institutions—accountants, lawyers, and real estate agents—to what are termed "custodian wallet providers" (entities that provide to hold, store, and transfer virtual currencies on behalf of customers) and "providers engaged in exchange services between virtual currencies and fiat currencies."

The EU was clear in the recitals to the new directive that it was expanding the scope of the regime to include cryptocurrencies because it feared that terrorist groups might be able to transfer money into the EU financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms.

Even as member states work to implement 5AMLD, the EU is now turning its attention to 6AMLD. Published on Nov. 12, 2018, this next iteration seeks to harmonize the enforcement regime across member states by setting out predicate offenses (which until now have been the purview of member states) and directing that all member states should ensure that the offenses are punishable by a maximum term of imprisonment of at least four years.

Given the complexity that these additional regulations add to the traditional AML/KYC legal framework, financial institutions and other entities with a global presence and potentially subject to these new requirements will need to think carefully about how their compliance programs reflect a careful understanding of these often-complex laws.

The Impact of New Technologies on AML Compliance

Potential Challenges Rooted in New Technology

While money laundering schemes have traditionally focused on disguising the use of traditional currencies involved in criminal or terrorist operations, the surge in popularity around virtual currencies has further complicated how AML risk must be assessed by financial institutions. New technologies have the potential to present new types or magnitudes of risks to businesses required to know their customers and maintain effective AML programs. One of the main appeals of virtual currency is varying levels of anonymity, which necessarily presents issues for financial institutions tasked with performing due diligence on customers and their business associates. Because virtual currencies are operated on decentralized systems, financial institutions can do very little to control the flow of assets, regulate how transactions occur, or stop problematic transactions.

However, the inherent characteristics of virtual currency and other blockchain-based activities are not the only sources of risk for AML programs. New forms of technology can also facilitate traditional criminal conduct, presenting challenges to developing effective AML compliance programs. Such difficulties include obstacles to screening parties, detecting red flags, and reporting suspicious activity.

For instance, although Bitcoin transactions are traceable through the blockchain, Bitcoin "mixers" or "tumblers"—additional anonymization technologies—can help obscure the transaction history, much like layering methods used in ordinary money laundering. Bitcoin ATMs have also arisen, providing opportunities for criminals to convert Bitcoin to cash without going through a registered institution required to identify the withdrawer. Combined with growing concerns that virtual currency is a growing means of funding terrorism and other criminal activity, these developments mean that financial institutions face significant and qualitatively different threats and challenges in AML.

Technological Opportunities for Enhancing Compliance

Though the risks associated with new technologies should influence how institutions develop, implement, and monitor the effectiveness of AML compliance programs, they do not paint the whole picture. The unprecedented technical capabilities of blockchain have generated interest across various sectors, but just as blockchain has opened a new world of financial transactions through the growth of virtual currencies, it and other emerging technologies hold promise in fintech to reshape AML programs.

Though blockchain-powered AML methods are in their infancy, they could soon be leveraged as powerful tools to detect and prevent money laundering. For example, the immutable characteristics of a blockchain ledger create reliability and consistency in developing a transactional history, while also allowing businesses and regulators to access a permanent and retraceable path of every transaction. Whereas cash is fungible and can trade hands anonymously, blockchain-based transactions can be reviewed and traced back to any suspect activity.

Even anonymous virtual currencies can be reviewed to detect passage through known addresses. Additionally, blockchain records are inherently cryptographically secure and, while not invincible to high-tech attacks, are not susceptible to traditional hacking methods. Whereas ordinary financial records could be compromised through countless physical and technical vulnerabilities, a sufficiently developed blockchain is more difficult to tamper with. Finally, because blockchain

data is distributed and not maintained under the control of a single entity, records can be reliable, cheap, and easily accessible across financial institutions and regulators.

In addition to blockchain, artificial intelligence and machine learning can augment AML programs by increasing the speed and efficiency of suspicious activity reporting and monitoring. In a Sept. 2018 speech, Serious Fraud Office director Osofsky remarked that the office's cases "are some of the most complex and data-heavy criminal investigations in any jurisdiction." She acknowledged that technology can help law enforcement keep up with the massive amounts of data in these investigations, and said that "we'll soon bring a range of machine learning and AI based technology assisted review features to our investigations … This should create even greater efficiencies, and potentially help us reach charging decisions sooner, and shorten the time it takes to progress to trial."

As these remarks indicate, managing, filtering, and evaluating alerts of suspicious transactions could be substantially enhanced and optimized by machine learning systems that can identify and prioritize suspicious activity, which will turn allow human reviewers to focus efforts on reviewing the most relevant alerts and supervising the system itself. By learning from a business's customer base and transaction types, these systems can bring red flags to the forefront and make data far more manageable. In addition, increasingly reliable systems for digital identities can also increase security while simultaneously reducing the amount of information that a financial institution needs to request from a customer.

These systems enhance data privacy and account security, and they can also serve AML objectives by helping businesses identify high-risk customers and allowing users to interact with financial institutions using identities that have already been trusted and/or verified. As a reflection of these promising characteristics, financial institutions in Europe have already begun implementing digital identity systems with positive results. These developments demonstrate how risks associated with new forms of technology can and should be balanced by evaluation of their potential to increase the effectiveness of AML compliance programs.

Conclusion

Recent and developing enforcement trends reflect a highly focused effort to root out financial institutions and individuals that fail to take AML compliance seriously. At the same time, the regulatory landscape continues to evolve and further complicate the AML/KYC legal framework. In dealing with these challenges, new technology offers both risk and promise for banks and other institutions seeking to develop and implement new strategies to improve AML compliance processes. In years to come, it will therefore be crucial to understand how technology, enforcement priorities, and new rules intersect in order to effectively respond to these rapid changes in the AML compliance landscape.

This article was written with the valuable assistance and contributions of Justin Kanji, a trainee solicitor in Ropes & Gray's London office.

