Briefing

Improving global AML efforts with technology and regulatory reform

November 29, 2017

Bart van Liebergen, Associate Policy Advisor, bvanliebergen@iif.com, +1 (202) 682 7447
Matt Ekberg, Senior Policy Advisor, mekberg@iif.com, +1 (202) 857 3622

- Despite enormous effort and investments from the financial and public sectors to detect and counter money laundering, illicit flows in the financial system are still significant, growing, and often moving undeterred.
- The difficulty of automatically detecting suspicious transactions and follow-up investigations are key issues for banks in compliance with anti-money laundering/counter terrorism financing ("AML/CFT") regulation.
- However, the deployment of new technology, combined with targeted regulatory reform could dramatically improve the effectiveness of the global AML/CFT system.
- New technologies including machine learning, digital identity, KYC utilities and distributed ledger technology (DLT, also called "blockchain") can improve compliance capabilities in the financial sector in a variety of ways, while regulatory reforms should address barriers to information sharing.

A version of this white paper appeared in "Financial Crime and Operational Security, Europe 2017," Clear Path Analysis UK, November 2017.

ISSUES IN CURRENT AML/CFT POLICY

There is a near-consensus that the current anti-money laundering (AML) and counter terrorism financing (CFT) framework is not as effective as necessary.[1] Every year, funds laundered through the global financial system equal an estimated two to five percent of global GDP, or 800 billion to 2 trillion US dollars. That percentage is still rising, especially for emerging economies. It is estimated that less than one percent of these criminal funds are being frozen or confiscated by law enforcement each year.[2]

This is not for a lack of effort. Banks are the eyes and ears of law enforcement in the global AML/CFT framework, identifying clients and understanding their source of wealth by applying stringent Know Your Customer (KYC) practices, and monitoring client activity and transactions on a continuous basis. Over the past several years, they have hired thousands of compliance staff to investigate suspected money laundering cases and file Suspicious Activity Reports (SARs) with regulators. In 2016, financial institutions (FIs) filed two million SARs at FinCEN, the US financial intelligence unit, alone. At the UK National Crime Agency, a half a million were filed. The available statistics show that SAR volumes are growing at a rate of approximately 11 percent per year (see fig. 1).[3]

However, the current framework for information gathering and reporting by the financial sector has not fully contributed to a better financial crime risk management infrastructure globally. For example, eighty to ninety percent of suspicious reporting is of no immediate value to active law enforcement investigations.[4]

The reasons for the relative ineffectiveness of the global compliance regime - in spite of the enormous effort of FIs to work as partners with law enforcement in the fight against criminal activity in the financial system - are complex, yet three interrelated key issues can be distinguished.

---

[1] See for example Terence C Halliday, Michael Levi and Peter Reuter, "Global surveillance of dirty money: assessing assessments of regimes to control money-laundering and combat the financing of terrorism," Center on Law and Globalization, January 30 2014.
[2] Figures from UNODC, "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes," 2011; and Global Financial Integrity, "Illicit financial flows from developing countries: 2004-2013," December 2015.
[3] Nick J. Maxwell and David Artingstall, "The role of financial information-sharing partnerships in the disruption of crime," Royal United Services Institute Occasional Paper, October 2017.
[4] Ibid.

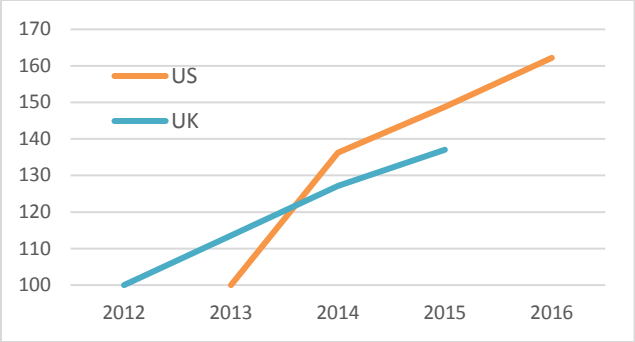

Fig. 1. Growth of SAR submission volumes at FIUs in the UK and US, 2012-2016 (1st year = 100%). Source: FinCEN, RUSI.

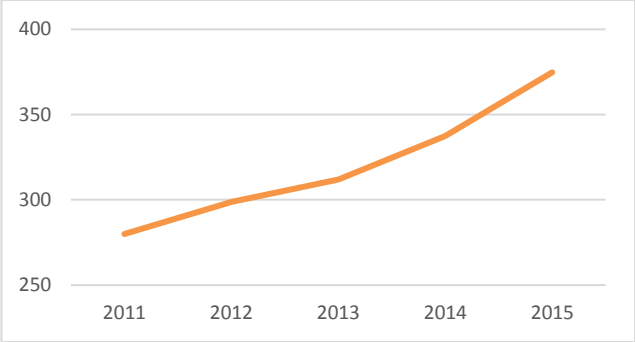

Fig. 2. Total number of payment transactions per year, in member jurisdictions of the Committee of Payments and Markets Infrastructures (CPMI), in billions. Source: CPMI.

First, FI transaction monitoring systems have so far been rather coarsely calibrated: about 95 percent of the alerts from these systems are so-called "false positives," or alerts that after closer investigation do not lead to a SAR filing. Compliance staff at FIs therefore spend a significant amount of time investigating transactions that should not have been flagged by these systems in the first place.

Second, the volume and variety of data on which AML investigations are based has made these processes difficult to automate. Data that needs to be assessed includes SWIFT messaging data, information from banks' internal client systems (such as personal and account information), credit card data, sanctions and watch list information, information retrieved from KYC utilities (repositories in which multiple institutions centrally share or store customer due diligence information), and other external data sources (news media and social networks, for example). A typical global bank conducts millions of transactions for its clients every month; transaction monitoring systems generate hundreds of thousands of alerts as a result. This volume of transactions and associated data is rapidly increasing (see fig. 2).

So far, the process of analyzing this information in AML investigations has been hard to automate due to the variety of data involved; instead requiring manual analysis. The sheer volume of information to be investigated has therefore led to a rapid rise in compliance staff numbers at banks, filing increasing numbers of SARs with FIUs (see fig. 1).

Third, the effective investigation of suspicious activity at banks is further complicated by barriers to information sharing. To obscure the illicit sources of their funds, money launderers typically move them across borders, across FIs, and across legal entities through various financial products. Yet restrictions on the sharing, storing or use of information, typically rooted in local regulation, make it difficult to gain or share information from other institutions or jurisdictions – or even from other subsidiaries within a bank's own group.[5]

At the Institute of International Finance (IIF), we believe that a combination of the deployment of new technology and regulatory reform could dramatically improve the functioning of the international AML/CFT system.[6]

TECHNOLOGY

In the last few years, FIs have increasingly deployed a number of leading edge technologies to improve compliance processes and risk management. Also called "regtech," some of them show significant promise in improving AML:

Machine learning can be applied to analyze all kinds of data sets, and typically shows improved predictive performance and accuracy over other types of analysis (such as conventional econometric modeling approaches). It is already being applied in AML with significant success. One goal is to improve the accuracy of transaction monitoring system alerts. Using various machine learning techniques, including clustering approaches and decision trees, banks can identify more complicated patterns of money laundering, and generate more refined customer risk segments, laundering scenarios and rules. One global bank achieved a

[5] IIF, "Financial Crime Information Sharing Survey Report," February 2017; IIF, "Facilitating effective sharing of AML/CFT information," May 2016.

[6] For an in-depth discussion of AML, technology and regulation, see IIF, "Deploying regtech against financial crime," March 2017.

26 percent reduction in false positives after applying machine learning to improve transactions monitoring. At the same time, it decreased its number of "false negatives": instances of suspicious activity that were previously *not* detected by monitoring systems.

Another application is the automation of (parts of) the investigations conducted following an alert. According to a head of AML at a global bank, analysts typically spend 80 percent of their time gathering information for those investigations, and just 20 percent on actual analysis.[7] Some machine learning-based systems automate this data gathering process, tapping into internal systems and external sources such as data repositories, social media and "deep web crawlers," and then pre-analyzing and structuring the information for the analysts' review.

One issue in training machine learning algorithms to recognize money laundering is that banks lack historical data on which of their filed SARs have turned out to be money laundering cases, and which didn't. This information would help train algorithms by letting them analyze the different traits of normal and illicit transactions. Lacking such labeled historical data, banks and vendors have achieved significant results by using unsupervised machine learning: using clustering approaches to create groups of transactions or clients based on similarities found by the algorithm. Also, supervised learning using "lower level SARs" as training labels has been used, training algorithms based on the distinctions between alerts that led banks to file a SAR, and those that didn't. However, these are still second-best options. For the best results, regulators should create a "feedback loop" reporting back to banks on which SARs were helpful, and which weren't.

As a key technology currently being implemented in AML, the IIF is currently mapping machine learning applications for AML at global institutions in more detail, with a report coming up early 2018.

Digital identity concerns the digitization of people's proof-of-identity and related personal information. The most well-known example of digital identity is India's Aadhaar project, through which more than a billion citizens have received a 12-digit unique-identity number based on their biometric and demographic data, giving them access to government and financial services.

Currently, banks spend considerable resources on identifying customers (for KYC and customer due diligence (CDD) purposes) and verifying their identities during onboarding. Generally, this is a cumbersome process involving a lot of paperwork; in many countries, customers are still required to identify themselves in person at a bank branch. Digital identity could streamline these processes for banks by automating these paper processes, while making onboarding or opening an account easier, more convenient and faster for consumers. For consumers in remote areas, digital identity would allow them to access financial services through phones or the internet, no longer requiring physical presence at a bank in their area. In AML investigations, it could help banks more quickly and reliably identify (parties to) a transaction or establish ultimate beneficial ownership, for example by attaching digital identifiers to financial transactions and instruments.

Blockchain* or *distributed ledger technology (DLT) seems to be further away from practical application as many aspects are still in development. In the longer term, it shows promise as a means to securely and instantaneously access and share information that could help solve some of the issues concerning information sharing between banks and law enforcement authorities.

DLT provides a single source of truth by requiring that any change in the database be verified by a majority of nodes, or entities that constantly update the database. This provides security, as a hacker would have to control a majority of the nodes in order to effectively manipulate the database. In time, KYC utilities could be placed on a distributed ledger, with participating financial institutions and law enforcement agencies acting as nodes. Logically, a permissioned distributed ledger would be the only option for this use case, as access to the database should be limited to entities with AML/KYC obligations under the Financial Action Task Force (FATF) framework.[8] DLT could also serve as a safe repository for unique identifiers for transactions, legal entities and clients.

[7] Comments at Sibos Conference, "AML and Assurance – Can Regtech define a better path?" Toronto 2017, https://youtu.be/T60lmJZBS-A.

[8] Credit Suisse, "RegTech: how a new wave of technologies is transforming the regulatory and compliance landscape for financial institutions," Washington White Paper, November 2016.

REGULATORY REFORM

As has been shown, new technology is being deployed by FIs with significant success to improve their effectiveness and efficiency detecting and countering money laundering, and has significant potential to attain further improvements in the future. However, to make the AML regime more effective, additional reforms are necessary particularly with respect to information sharing and the implementation and use of new technology at FIs.[9]

Information sharing between financial institutions, intra-institution and between the private sector and governments domestically and across borders should become much faster and easier. To that end, FATF should work to improve the effectiveness of its member states' information sharing regimes, specifically by including clear and enforceable standards on information sharing in the FATF Recommendations.[10] A greater focus should also be placed on enhancing national and multilateral programs for the financial sector and governments to exchange and analyze intelligence to prevent, detect and disrupt money laundering. In general, data regulations should become more risk-based: maintaining barriers to the sharing of sensitive personal information for commercial purposes, while creating more possibilities for FIs to share information with a national security- or law enforcement purpose.[11]

- A "feedback loop," created by law enforcement authorities such as financial intelligence units (FIUs) should allow financial institutions to learn how they can most effectively detect and report suspicious activity. Such information sharing from law enforcement back to the private sector could have multiple forms.
- A more flexible regulatory environment for FIs to apply transaction alert rules based on proprietary (for example, machine learning-based), supervisor-checked analysis.
- Improving data formats and standardization, for example by including digital identity-related information in the future.
- Barriers to digital identity, including for instance the requirement for consumers to identify themselves in-person during onboarding, should be reevaluated.

CONCLUSION

A two-pronged approach of deploying new technology and achieving internationally consistent regulatory reform should lead to a significant improvement of the international AML/CFT compliance framework. The ability of current technologies to analyze various sources of information, unambiguously identify clients, and improve information sharing provides an opportunity that should not be disregarded by the public and private sectors. A key point is that the deployment of technology is not merely a cost-cutting or efficiency exercise for FIs – it has systemic benefits in promoting improved tracing and countering of illicit financial flows.

Regulators and supervisors can support this development through a wide range of reforms and supportive supervisory practices. Given the global, cross-border nature of money laundering, improving the ability to share information among and within institutions, with governments and across borders will be key, but there are additional measures outlined in this article that will allow them specifically to support the effective deployment of technology. With money laundering flows totaling 5 percent of global GDP, and less than 1 percent of those frozen or confiscated, we can't waste a day.

[9] For more information on regulatory recommendations for improving the AML/CFT framework and supporting the implementation of new technology for AML, see IIF, "Deploying regtech against financial crime," March 2017.
[10] Ibid.
[11] For more information on the IIF's recommendations on information sharing for AML purposes, see IIF, "Financial Crime Information Sharing Survey Report," February 2017; and Nick J. Maxwell and David Artingstall, "The role of financial information-sharing partnerships in the disruption of crime," Royal United Services Institute Occasional Paper, October 2017.