NICE · ACTIMIZE

Intelligent Automation for Effective AML

Modernising AML monitoring programmes to ensure compliance with heightened regulatory expectations

Whitepaper
April 2019

Regulation Asia

Intelligent Automation for Effective AML

Financial institutions need to modernise their AML monitoring programmes to protect themselves and meet increasingly demanding regulatory expectations.

Financial crime has been growing steadily in recent years, and multiple factors are to blame. Global economic uncertainty, the rise in organised crime, and the relative anonymity of online and mobile commerce are a few of the reasons why banks face increased risk from financial crime.

The annual cost of financial crime to the global economy is estimated at US$1.45 trillion – US$166 billion in Asia Pacific – according to the 2018 Thomson Reuters True Cost of Financial Crime report. In Singapore last year, more than one-third of organisations reported being a victim of economic crime over the previous two years, 20% of which was said to have involved anti-money laundering (AML) incidents.

The challenge for financial institutions is that they are hamstrung by fragmented, mostly manual approaches

However, the actual cost of financial crime extends far beyond mere economic loss, as it impacts the lives of countless individuals and communities daily. As financial crime flourishes, bad actors are becoming increasingly sophisticated in their approach to finding new weaknesses in company defences, including through the use of automation.

The challenge for financial institutions is that they are hamstrung by fragmented, mostly manual approaches, forced to work with inefficient legacy systems and often overlapping tools. Between workflow prioritisation, evidence gathering and decision-making – institutions continue to lag as they struggle to work across departments and pull information from disparate sources. Mostly manual activities that span multiple departments, channels and data sources can easily result in detection failures, and this leaves organisations vulnerable.

However, since 2018, financial institutions have increasingly recognised that a better way was needed to manage financial crime risk. In the year ahead, financial institutions will have to work harder and smarter, with the help of technology, to safeguard their customers and block out bad actors.

We anticipate six core themes will emerge in 2019:

1. A stricter regulatory landscape, with priorities shifting towards increased supervision and rule refinement, and greater pressure from global frameworks;

2. Greater use of artificial intelligence (AI) and machine learning (ML) technologies to increase efficiency and effectiveness in red flag reporting and investigations;

3. Greater use of automation to reduce the manual processes that are currently overstretching compliance teams so they can instead focus on actual casework;

4. Greater use of segmentation and anomaly detection modelling to identify behavioural patterns commonly associated with suspicious activity and transactions;

5. Continued investment in people, not just machines, as institutions move towards technology-oriented approaches; and

6. Greater focus on individual and senior management accountability, where regulators are likely use new accountability regimes to make a few examples.

Historically, criminal networks have exploited the lack of inter-institutional communication by laundering money where detection was less likely

A stricter regulatory landscape

Few would doubt that the regulatory landscape has changed significantly around the world in the past decade. In recent years, regulators have repeatedly amended rules as their focus expanded from organised crime to countering terrorism financing (CTF). Governments have also developed their use of economic sanctions as an extension of foreign policy, shifting from pursuing countries to directly targeting individuals and corporate entities.

Unlike trends across the broader financial regulation landscape, which have seen a shift away from global policymaking towards more pronounced divergences in activity-based rules and fragmentation across jurisdictions, increased international cooperation and rule standardisation will continue to be a priority in the fight against money laundering.

Historically, criminal networks have exploited the lack of inter-institutional communication by laundering money through countries or banks where they were less likely to be detected. However, regulators in individual jurisdictions now have better defined global frameworks to rely upon – adding to pressures from local governments – which will enable them to better supervise regulated entities and address financial crime risk.

For example, Europe's Fifth Anti-Money Laundering Directive (5AMLD) will make beneficial ownership information publicly accessible and strengthen cooperation and the exchange of information between EU member states. Additionally, the extensive work of the FATF is expected to tighten loopholes that have allowed financial crime to persist, such as new rule recommendations in relation to professional services providers and the virtual asset sector.

In Asia, there has also been an increased focus on multi-agency cooperation and information exchange

Rather than change AML rules significantly, regulatory bodies in Asia are more likely to focus on how to refine existing domestic frameworks to ensure they meet internationally-defined standards, such as those under 5AMLD – required for doing business with Europe – and the FATF, whose praise and recognition is much-desired by regulators in the region.

In Asia, there has also been an increased focus on multi-agency cooperation and information exchange. This is reflected by the ACIP (AML/CFT Industry Partnership) in Singapore and the FMLIT (Fraud and Money Laundering Intelligence Taskforce) in Hong Kong, which both seek to enhance communication between financial institutions, law enforcement and other government agencies in relation to money laundering prevention and investigations.

At the same time, penalties for money laundering have increased. Under a new bill in Singapore, corporations found guilty of AML offences will have to pay the higher of SG$1 million or twice the value of the transactions in question. Failures to disclose information that might help prevent a terrorism financing offence or lead to an arrest, prosecution or conviction now also have stronger penalties.

A better model for red flag reporting

Still, 1.2 billion transactions take place in the global financial system every day. Spotting individuals connected to a crime is difficult, especially when transactions take place in a fraction of a second and are then followed almost instantaneously by layers of related transactions. Traditionally, banks have responded to these trends by investing heavily in manual controls and systems to address point-in-time needs.

But institutions recognise the need for a new approach, and that better technology and intelligent automation tools are the answer. The Monetary Authority of Singapore (MAS) has been pushing for greater use of data analytics to sieve through large volumes of data to identify and prevent financial crime. The regulator is already using such technologies to analyse networks of suspicious transactions, conduct supervisory probes and examine higher risk activities.

Indeed, a November 2018 paper from ACIP identified a number of the key weaknesses of current AML/CFT approaches at financial institutions, including high false positives in name screening and transaction monitoring, rapidly-changing typologies, and excessive manual processes in decision-making which can result in inconsistencies and human error. But, according to the paper, Singapore banks have already been deploying data analytics solutions to address these weaknesses.

In one case, a bank was reported to have achieved 50-60% reduction in name screening false positives, a 40% reduction while the transaction monitoring false positives, and a 5% increase in true positives through AI-enhanced data analytics techniques. In another case, a bank reported double-digit efficiency gains in operational processes related to the detection of financial crime.

Assisting overstretched compliance teams

...the use of AI, ML and other automation tools will focus attention on real cases that require immediate attention

By helping to more effectively filter out false positives and enhance efficiency, the use of AI, ML and other automation tools will allow compliance professionals and investigators to focus on real cases that require their immediate attention. Investigators are still currently spending 80% of their time preparing cases, and only 20% analysing data. Some AML teams are spending up to 90% of their time on manual tasks, which leaves fewer resources to recognise changes in customer behavior and run efficient investigations.

This year, financial institutions will refocus their attention on AI's current capablities. In financial crime management, the focus will be on areas where costs can be lowered, risks can be reduced and more efficient operations can be enabled. Reducing human intervention will be key in all these areas.

Technologies such as AI and ML not only have the potential to minimise manual processes, they can also streamline many of the repetitive tasks that will remain after much of the automation has taken place – tasks that continue to weigh down compliance and operations teams. In addition to alleviating the cost and time burden, these technologies make compliance a more meaningful exercise.

Segmentation and anomaly detection to take centre stage

Although AI will help in financial crime detection, data will be a key diffrentiator in the year ahead, and institutions will continue to seek out new ways to handle the large, cumbersome and multi-dimensional data sets, with metrics that stretch across millions of rows.

More important will be the ability of analytics techniques to use various parameters – such as user behaviour, conversion patterns, historical traits and other risk characteristics – to reveal patterns between intra- and inter-acting entities that are part of cohesive groups.

In Hong Kong, the SFC (Securities and Futures Commission) has gone on record saying that one of the most difficult problems facing the market is what the regulator refers to as "nefarious networks". These groups use their control over listed companies to enrich themselves at the expense of unsuspecting investors by coordinating their activities behind seemingly legitimate entities. The SFC is developing data and intelligence tools to help it better identify these groups.

Data-sharing capabilities can help make identifying potential criminal behaviour easier and less of a cost burden for institutions

In the year ahead, the handling of any large data sets for AML purposes will require segmentation and anomaly detection technology. Segmentation of customers enables more effective analysis against historical transactions and peer group activity to identify behaviours that are outside expected norms – this serves to enhance existing AML monitoring programmes.

However, persistent issues related to data sharing will continue to frustrate institutions, including a lack of cooperation between internal teams, limited access to external data sources, and legal constraints on what banks can share with subsidiaries, other banks and law enforcement. These challenges are likely to remain in 2019, as most jurisdictions look to beef up their data privacy regimes rather than relax them.

Further, the quality of data and what banks can do with it will continue to be problems until regulators in Asia Pacific have a change in mindset in terms of how they see data-sharing restrictions as hindrances in AML compliance processes. Data-sharing capabilities can in fact help make identifying potential criminal behaviour easier and less of a cost burden for institutions, while also enabling them to more proactively prevent illegal activity in the first place.

As an example, the Reserve Bank of India (RBI) is requiring all payment companies to store their data only in India so it has "unfettered supervisory access". Several multinational firms, most notably Mastercard, have lobbied for the RBI to soften its stance on data localisation, arguing that such requirements severely impact their global fraud defences.

Continued investment in people, not just machines

Despite the proven benefits of AI, recent research from PwC focusing on financial crime capabilities has found that most financial institutions are is still lagging in their readiness to adopt such technologies. The research found that business leaders are not sure where to start, or, conversely, thinking too far ahead to techniques that are feasible but not practical yet.

...we will start to see a true partnership between machines and humans, collaborating to accomplish things that neither could do as well on their own

Notably, tools and models based on AI technology, no matter how intelligent, cannot be expected to operate without human oversight and testing. Even in the case of unsupervised learning, humans with subject-matter expertise must design and optimise the models. Business leaders will need access to technical expertise to help them determine the best path forward if they are to move ahead with implementing new technologies.

In the year ahead, we will start to see a true partnership between machines and humans, collaborating to accomplish things that neither could do as well on their own. With this in mind, financial institutions and regulators alike are expected to continue investing in more effective approaches for ensuring staff are adequately skilled and kept up to speed on the latest techniques used by bad actors.

As the fight against financial crime shifts towards more technology-led approaches, there will be a higher demand for related skill sets. Facing a looming skills-gap, financial institutions will have to upskill existing staff and seek out new hires to ensure a minimum level of technical competence.

A recent paper from Singapore's ACIP cited a shortage of skilled data analysts to help banks track down illicit cash flows. The paper said importing foreign talent and training existing employees could help to address the challenge, but it is also likely that banks will rely on specialist partners to help them meet the skills gap.

Demands for accountability

Bad news travels fast, and there has been a pronounced shift in the way the world looks at fraud, corruption and financial crime over the past few years. In 2019, increasing expectations from regulators will force financial institutions to adopt principles-based approaches which emphasise better governance, organisational culture improvements and increased accountability when things go wrong.

Such developments were made evident in Australia, where fallout from the Royal Commission into financial sector misconduct will likely force authorities to make examples of executives for the failings of their institutions under the Banking Executive Accountability Regime (BEAR). The new regime came into force for large institutions in July 2018 and will bring into scope small and medium institutions in July 2019.

The new accountability regimes place a greater onus on financial institutions to strengthen their AML controls and risk management processes

Following the Royal Commission, the Australian Prudential Regulation Authority (APRA) announced plans to both extend BEAR to cover the insurance and superannuation sectors, and to also broaden its scope to increase focus on conduct matters. The regulator is also reviewing its enforcement approach in light of the new accountability regime.

In Singapore, the MAS released guidelines in April 2018 aimed at strengthening individual accountability of senior managers and setting out regulatory expectations with respect to individual conduct. The guidelines also sought to strengthen oversight of employees in material risk functions, including in areas such as AML.

Meanwhile in Hong Kong, the SFC introduced the Manager-in-Charge (MIC) regime in 2016, making managers responsible and accountable for the conduct and behavior of those they oversee. The Hong Kong Monetary Authority (HKMA) has likewise introduced a management accountability initiative for banks, and all indications suggest it plans to hold the individuals responsible for key middle and back office functions (including AML and compliance) to account when things go wrong under their watch.

The new accountability regimes place a greater onus on financial institutions to make sure their AML controls and risk management processes are up to standard, and operating with high levels of efficiency and effectiveness. And it is precisely because these regimes are new that regulators will be looking to make a few examples of those they believe have fallen behind.

Time to take action

The current approaches to combatting financial crime have not kept pace with modern techniques used by criminal organisations. There is a real need for change through innovation, and in 2019 financial institutions can no longer afford to ignore newer technologies in favour of more traditional approaches.

Smarter technologies such as AI, ML and other automation tools can not only drive efficiencies when applied to existing workstreams, but they can also help to identify new and creative ways to tackle financial crime. Ultimately, such tools enable institutions to better safeguard their customers and block out bad actors. But, the adoption of ML, AI, and other automation technologies will continue to pose challenges for banks and test institutional risk appetites. Financial institutions will need to leverage on specialist partners to implement the right strategies to ensure a smooth transition to newer technologies.

NICE Actimize is one company that is helping financial institutions apply AI-enhanced automation to the process of gathering data from disparate sources and to perform some steps in AML investigations, thereby enabling more efficient alerting and reporting, as well as better resource allocation to the risk areas that need it most.

The firm has been reshaping the AML landscape by incorporating transformative technology in the space – from how financial institutions manage their data and apply analytics to data sets, to workflow optimisation and behaviour pattern recognition. NICE Actimize aims to ensure that organisations are able to protect themselves, their reputations and their customers.

Unifying financial crime, risk and compliance programmes through AI-enhanced automation helps to drive operational efficiencies, and ML improves the process with each investigation.

To find out more, visit https://www.regulationasia.com/effective-aml/ for access to a joint webinar hosted by Regulation Asia and NICE Actimize.

NICE · ACTIMIZE

Get in touch www.niceactimize.com

Regulation Asia

www.regulationasia.com