BANKING INSIGHTS

BAE SYSTEMS

From FRAML to Unified FinCrime

How to define a long term strategy

Not only has society the world over been busy fighting rising levels of COVID, but businesses have also been faced with rising levels of opportunist criminals praying on vulnerabilities during the pandemic. In fact, our COVID Crime Index revealed that 74 per cent of financial institutions (FIs) in the UK and US experienced a significant spike in threats linked to COVID-19.

In tandem, financial institutions (FIs) across both markets have also been faced with the need to cut IT security, cyber crime, fraud or risk department budgets by almost a third (26 per cent) in the past 12 months[1]. While there isn't a direct connection, this mirrors the criminal activity detected by FIs that had also risen by a third (29 per cent) since the start of the pandemic and a further 42 per cent of FIs said that the remote working model due to COVID-19 makes them less secure.

Historic hurdles

While these findings are major factors for FIs as they look at the year ahead and review their financial crime (FinCrime) strategy, they are also faced with the ongoing impact of the pandemic. Such factors have only exacerbated existing issues that pre-date the pandemic. Banks have long been faced with rising rates of fraud and cyber crime, regulatory hurdles and increasing operating costs, with the undeniable need to protect customers and safeguard their reputation and operations.

The ability to manage FinCrime is impeded by the lack of available skilled staff, siloed departments, lack of collaboration and limitations of legacy IT. However, the impact of these issues runs deeper than the immediate concerns regarding customer protection. Banks are struggling to deal with the resulting overwhelming workloads and volumes of false positives due to the narrow visibility afforded to each silo, all while trying to ensure a positive customer experience. Fraudsters thrive when data silos exist, and with many banks continuing to struggle with legal IT and siloed data, this is a particular threat.

Fraudsters thrive when data silos exist

Best intentions for synergies

Such challenges, both historic and those newly introduced or exacerbated by the pandemic, are pushing banks to breaking point. Banks are looking to drive synergies between fraud, cyber and compliance functions to tackle FinCrime hurdles. Currently only a quarter of retail banks have adopted an integrated approach to FinCrime systems, yet active collaboration between functions is now becoming the norm, according to a report by Ovum.

The report also found that 70 per cent of banks are looking to achieve synergies within the next three years and that North American banks are typically more mature in their approach to tackling financial crime, driven by the strength of technology platforms. The report highlighted that the "key challenges with existing technology platforms are adaptability and speed, with banks looking to artificial intelligence (AI) to improve effectiveness in both AML compliance and combating fraud". Overall, demonstrating a clear gap between those that have acted on their desire to adopt an integrated approach to FinCrime, and those that still have some way to go.

Unified FinCrime strategies

Many banks have the best intentions, but with the combination of reduced budget, reduced resources, lack of visibility and rising rates of FinCrime, not all current solutions and strategies banks have in place are best placed to meet modern demands. This is where a unified FinCrime strategy that encompasses anti-money laundering (AML), cyber threat intelligence, regulatory compliance, transaction monitoring, watchlist screening and monitoring for PEP and Sanctions (WLM), know your customer (KYC)/customer due diligence (CDD) processes and fraud detection all have a key role to play. As AML, cyber and fraud teams all use pattern and behavioural anomaly identification, it makes sense to break down operational silos and establish a collaborative approach that creates an efficient, effective and successful environment. This can reduce the costs of data integration, model development, and investigative efforts company-wide.

In order to embrace a Unified FinCrime strategy, banks must work with each of these traditional teams to assess synergies, identify nuances and implement a strategy that focuses on the people, processes and technology, which we will now explore.

Processes

In order for a new unified FinCrime division to truly work, processes and ways of working between specialist areas will need to be reviewed. Data migration and data sharing will be of utmost importance here. KYC/CDD/transaction history/WLM data is all valuable to fraud detection and fraud investigations. Having a customer's historic information accessible at the click of a button enables fraud teams to identify unusual behaviours early on, and even identify smaller cases of fraud that may signify a larger case of money laundering.

However, some banks may have very conservative policies regarding data sharing and will not share data outside of compliance teams, while others are more willing to share legally permitted information with other FinCrime units of their institution. If investigators outside of compliance have full access to data, this insight can be invaluable to reducing fraud, tackling money laundering, and improving compliance in the long run. Of course, there needs to be precautions in place surrounding high profile and internal cases that still need to be protected. But, for example, if cyber threat information is integrated with transactional history and accessible to fraud teams, fraud teams can identify if a flagged fraudulent transaction may be due to a customer's data being compromised following a larger data breach, or whether it could be an indicator of a victim of labour exploitation or drug trafficking. Both of which are equally important factors behind a potentially fraudulent transaction that fraud teams need to be aware of.

People

One of the biggest hurdles to adopting change is internal politics, deep-set habits, differing business objectives and regulatory regimes. In order to embrace a new strategy, a total combined team effort and collaboration is required to break down legacy siloes and work together towards a common goal.

For collaboration to be possible, each of the siloed departments will need to come together to make a unified FinCrime division in order to see themselves as one combined team and enable ad-hoc sharing and information collaboration. However for this model to be successful new ways of working to address FinCrime will need to be driven from the top down and embraced by the entire team.

Dependencies will also need to be identified between groups, such as how can fraud and AML investigators work together. There may also need to be consideration for a compliance specialist to be embedded within fraud teams to scrub-up fraud claims to check for AML, and vice versa for AML compliance. This is likely to influence a team restructure where you have a dedicated FinCrime director, for instance, with speciality managers for each area of expertise that all report into the FinCrime director. Training and team building efforts will likely be required to reinforce unified working and collaboration between each groups.

Technology

There is evidence that fraudsters are already using sophisticated techniques so rules alone are insufficient and lack agility for new channels, especially as criminals pray on siloes. Automating data sharing and insights between these siloes will help define a unified strategy, tackle FinCrime and ensure a frictionless way to establish a holistic customer view. New technologies, such as machine learning can help in this scenario by automating data processes, but it can only be as good as the data it is fed.

Detection techniques for both fraud and AML are based around data pattern recognition that is increasingly reliant on artificial intelligence (AI) and analytics for improved analysis and decision making. By automating the collection, standardisation, digestion and sharing of data through a centralised platform all areas of unified FinCrime team are afforded a centralised view of the alerts and incidents flagged. This also reduces overheads, false positives and the potential for human error associated with the manual sharing of intelligence and allows for such data to be processed in real-time.

With a centralised view, investigators can spend time on high-value analysis, rather than low value data gathering. This is all possible through the unified central platform that brings in a high-volume of internal and 3rd party data sources.

How can this aid each specialist area in the FinCrime division?

Take AML, for example. In the past, AML primarily involved the batch-sorting of transactions at the end of each working day. This approach was based on looking at a customer's behaviour against known money laundering typologies. Now, customers can open an account online, move funds and close it down, all in a matter of hours and before traditional batch-sorting could identify and alert.

Real time transaction monitoring through a centralised platform could intervene and prevent this from occurring – but it highlights the differences between money laundering and fraud. The current objective of existing AML surveillance is not to prevent activity. Instead, the aim is to report activity so that financial investigators can trace the flow of funds across institutions.

If these steps to creating a unified FinCrime strategy are taken, banks will stand to benefit from improved collaboration, efficiency and effectiveness with a 360° customer visibility that in turn drastically reduces false positives and increases detection accuracy. This is enabled through confident collaboration via consolidated alerts, evidence and financial metrics stored within a single platform, as well as the ability to retain closed cases indefinitely or for as long as audit standards require. With aggregated risk indicators shared across source systems, investigators are presented with a holistic view to focus on analysis rather than data gathering. And ultimately, with investigation data presented in a logical way, instructional design techniques can be leveraged to simplify and accelerate decision making. All of this is made possible through the banks new central platform that brings in all previously siloed data sources.

Conclusion

The industry has become accustomed to the term FRAML that encompasses both fraud and AML strategies and operations. However, this strategy isn't far reaching enough. The key to tackling FinCrime lies in data, and it isn't just the fraud and AML teams that can benefit from data collaboration. A unified FinCrime strategy takes banks from viewing crime through the isolated lenses of the fraud and AML teams, and opens their view up to all customer touch points within an organisation. The more siloed systems that are brought together, the more malicious criminals are stopped in their tracks that pray on disjointed processes.

In the next five years we can expect unified FinCrime strategies to become common practise, and some are already starting to introduce aspects of this approach in response to business and customer demands. Some banks have started to embed investigators within each of the siloed teams or referral processes, and instigate training around compliance issues for wider teams. Smaller Credit Unions, institutions and FinTechs are more likely to already have aspects of cross AML and fraud teams in action due to the need for individuals to cover multiple responsibilities as business grows. However, in reality, bigger banks may be slower to adapt due to the sheer size of their teams.

Looking for a Unified FinCrime solution?

NetReveal from BAE Systems spans the entire financial crime, risk and compliance functions, centralising alerts and incidents into one enterprise-wide investigation platform. Alerts are pre-processed, enriched and routed automatically. As a consequence, investigators spend time on high-value analysis, rather than low value data gathering. This is all possible through the unified central platform that brings in a high-volume of internal and 3rd party data sources.

Click here to find out more about

NR NetReveal®

[1] https://www.baesystems.com/en-financialservices/insights/the-covid-crime-index

BAE SYSTEMS

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/bankinginsights