Combatting financial crime: Panel summary

Experts discuss potential benefits of applying a joined-up approach to anti-fraud and AML, and of machine learning technology.

Contents

Executive Summary

Panelists

Ben Hargreaves
Director, Global Head of Anti-Fraud, Credit Suisse.

Ben has spent more than 20 years working with and for financial services providers in the fields of fraud, credit and financial crime risk.

Cate Kemp
Group Payments Compliance Director, Lloyds Banking Group.

Cate established – and now heads up – the group's Compliance Shared Services for AML, Sanctions and FATCA.

Jeremy Warren
Managing Director, Head of CIB Global Financial Crimes Compliance, J.P. Morgan.

Angus Wildblood
Partner, Risk Advisory, Deloitte.

Angus uses insights gained from data analytics to help banks address regulatory challenges including AML and sanctions.

Session highlights

- Anti-fraud and AML departments have a number of data points in common.
- Bringing AML and anti-fraud practices closer together can lead to better customer protection and faster onboarding.
- However, achieving a joined-up approach takes time, money and effort.
- There is a greater focus on working together to prevent and detect financial crime.

Fraud and AML:
A Joined-Up Approach

Most institutions separate their anti-fraud and AML teams, even though both disciplines have very similar objectives, face similar challenges and use similar tools and processes. In light of this overlap, a more joined-up approach could provide considerable benefits. This was the focus of a panel discussion between industry experts at Sibos 2016.

Common ground

The experts pointed out that anti-fraud and AML departments focus on a number of common data points when assessing different types of financial crime activity, such as the origin of a transaction, the beneficiary, the destination and whether a transaction constitutes normal behaviour.

One panellist illustrated this overlap by citing the example of a client who instructs a bank to pay the director of a trust fund into a personal account in a high-risk jurisdiction. The transaction relates to the purchase of precious metals, and a customs agent is involved. As the panellist explained, “When you start to think about a transaction like that, is it potentially fraud? Is the client being defrauded, or are they participating in some sort of fraud ring? Is it a potential AML issue, or a potential bribery or corruption issue?”

The expert added that verifying the different components of risk point by point does not result in the best client experience. Instead, the components of risk need to be considered from a unified point of view in order to make the right decision with a one touch approach from the point of view of the client’s experience.

Indeed, the panel noted that bringing anti-fraud and AML closer together could result in a number of benefits, including better customer protection and a streamlined process for new customers joining a bank. Nevertheless, opinions varied about how to achieve this. One of the panellists said that their joined-up approach involved client education and having more client outreach covering both areas at the same time. Another said that opportunities for a joined-up approach could be found in the area of investigations case management.

Considerations

While a joined-up approach offers clear benefits, the panellists made it clear that achieving this is not necessarily straightforward. One expert noted that the consequences of bringing anti-fraud and AML practices together could be unpredictable. For example, customers who had been informed they could be the victim of a scam had complained about the intervention and had wanted to proceed with planned payments.

The panel also pointed out that despite the overlaps, there are still some notable differences between anti-fraud and AML. For one thing, anti-fraud and AML may have different objectives. Whereas the focus of anti-fraud is risk management, AML is more about managing compliance and one’s standing with regulators.

As such, the timings of any intervention may differ: a timely intervention is more important when a bank is seeking to prevent a fraudulent transaction from taking place, whereas compliance actions can be batched up and saved for later.

On another note, the panel pointed out that joining up AML and anti-fraud takes time, effort and investment – and that cross-functional training is needed if people are to look at financial crime holistically, rather than making siloed decisions about a particular type of crime risk.

“

The underlying infrastructure, the technology, the kinds of data you’re using, the viewpoints that you are trying to get to – they are very much in common.

Ben Hargreaves
Director, Global Head of Anti-Fraud,
Credit Suisse

“

One of the luxuries we’ve had at Sibos is we’ve had both teams here in front of the clients talking about AML and fraud. There’s been a lot of benefit and synergy between those two.

Jeremy Warren
Managing Director, Head of CIB Global
Financial Crimes Compliance, J.P. Morgan

Regulation

The panel also discussed regulation and whether a different approach would be needed to support the convergence of the two areas. According to one expert, regulators are beginning to entertain such changes – but this is at a very early stage. Others pointed out that while the regulators set certain minimum standards, banks have a responsibility over and above that to use all available capabilities, intelligence and tools to combat financial crime.

Collaboration

The experts noted that preventing and detecting social harm is not a competitive topic, and that there is a greater focus on working together to understand how best to prevent and detect financial crime. The panellists said that KYC utilities can play a role in supporting KYC activities by acting as a repository for information and saving time and effort.

Beyond this, collaboration could play a role when it comes to combining intelligence. One expert pointed out that even if individual banks have strong processes in place, criminals could use relationships with multiple banks to conduct illicit activity while "making things look completely clean within one entity". The challenge therefore lies in bringing the necessary intelligence together across institutions as well as between AML and anti-fraud departments.

Conclusion

Finally, the panellists were asked what they would do differently if they had the opportunity to set up their financial crime compliance functions from scratch. They said that this would depend on the type and size of the institution in question. However, one approach could be to adopt a common platform and shape the organisation around the technology.

One of the experts commented that their starting point would be moving from 'I think' to 'I know' – in other words, taking the time to understand how different areas operate and figuring out how best to align them. Another said that instead of having separate people in charge of fraud and AML, it would be preferable to have one person in charge of financial crime, with teams reporting into them.

> **I think if we leave it to regulators and regulation, we will not end up with the world we all want.**
>
> **Cate Kemp**
> Group Payments Compliance Director,
> Lloyds Banking Group

> **Particularly in some businesses, AML is a bit like looking for a needle in a haystack. You know you found some needles, but you don't know whether you found all of them.**
>
> **Angus Wildblood**
> Partner, Risk Advisory, Deloitte

Machine Learning – The Future of Compliance?

Meanwhile the technology available to help banks tackle financial crime is also evolving – as highlighted by another session at Sibos exploring the role that machine learning can play in compliance.

The experts explained that machine learning is a subset of artificial intelligence (AI) which enables machines to detect patterns and make decisions accordingly. While this technology is in its infancy where banking is concerned, compliance is a particularly interesting area of focus. Machine learning is being used by banks for areas ranging from high-end investigations through to KYC at the onboarding stage.

As one of the experts said, a lot of time is currently spent on false positives. The benefit of this type of technology is that it can recognise patterns in order to discard false positives and focus on the genuine risks.

The challenges for this technology lie not just in identifying unusual transactions but also in being able to explain why transactions have been identified. The latter is a particular area of focus, with one of the experts highlighting the benefits of working with human investigators to capture knowledge.

> **Your best customer looks very similar to the best criminal, and the difference between the two is a very thin line.**
>
> **Nick F. Ryman-Tubb**
> CEO, Institute of Financial Innovation inTransactions & Security

Panelists

Dan Adamson
Founder & CEO, Outside Intelligence, Inc.

Before founding OutsideIQ in 2010, Dan was previously a technical lead at Microsoft for the Bing Health search team and Health Solutions Search.

Nick F. Ryman-Tubb
CEO, Institute of Financial Innovation in Transactions & Security.

Nick is currently creating a world-leading secure payment fraud laboratory working with the industry and leading universities.

Anthony Fenwick
Global Head of AML, Citi.

Anthony has led a number of major compliance infrastructure development and implementation projects, including Citi's OneKYC programme.

Session highlights

- Machine learning is being used by banks for high-end investigations as well as for KYC.
- In the context of compliance, machine learning can be used to achieve time, efficiency and productivity improvements.
- The panel reported that regulators are supportive of machine learning – but that they are also looking to banks to explain how the technology can be used.

Other considerations

The following points were also discussed:

- **NLP.** The experts explained that natural language processing (NLP) is the ability to understand written or spoken human language. This is a difficult field where compliance is concerned, due to the global nature of the topic.

- **Sustainability.** Banks are solving regulatory problems by recruiting larger numbers of people in compliance, but this results in higher costs. The question is how automation can be used to make this effort more efficient and sustainable.

- **Low-hanging fruit.** The panellists were asked which areas offer opportunities for early success. One expert suggested that it may be valuable to choose a small subset of the cash monitoring business in order to prove the worth of technology in the process.

- **Data quality.** One of the experts noted that data presents a considerable challenge for many different projects. Where machine learning is concerned, the goal should be to obtain a mixture of customer-side data and transactional data from across the bank. However, he added that perfect data is not essential for machine learning.

- **Risks.** The panel said there is a risk that the bank's monitoring system is a "black box in the corner" which no one understands. It is important to keep well-trained, experienced investigators working with the technology.

Building a business case

When it comes to building a business case, the panellists noted that key performance indicators include time, efficiency and productivity gains. In order to be attractive, machine learning needs to be more effective than existing processes.

The panel also mentioned that getting the necessary attention from IT can be a challenge. If the IT group already has projects planned for the next 18 months, getting buy-in for a machine learning solution may not be straightforward. In some cases it may be advisable to get a smaller system in place in the first instance, which can work alongside existing systems.

When it comes to choosing an appropriate partner, the panellists said that innovative new technology should not be the only consideration – it is also important to work with world-class AML experts. The experts also said that banks should look for a suitable level of support, which may mean opting for a slightly more established system.

Regulators

Finally, the panellists discussed where regulators stand on this type of technology. One expert said that different regulators around the world may approach this technology differently, but that regulators are largely supportive. However, the panel also said that regulators are, to a certain extent, relying on larger organisations to explain what they are planning to do with this technology.

Conclusion

The panel concluded that while compliance continues to present major challenges for financial institutions around the world, the industry is working to increase the efficiency of the associated challenges. Leveraging machine learning and adopting a more holistic approach to anti-fraud and AML are two ways in which institutions may be able to overcome their current challenges and achieve efficiency gains.

About SWIFT

For more than 40 years, SWIFT has helped the industry address many of its biggest challenges. As a global member-owned cooperative and the world's leading provider of secure financial messaging services, we enable more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, relentlessly pursue operational excellence, and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. We also bring the financial community together to work collaboratively to shape market practice, define standards and debate issues of mutual interest.

SWIFT users face unprecedented pressure to comply with regulatory obligations, particularly in relation to the detection and prevention of financial crime. In response, we have developed community-based solutions that address effectiveness and efficiency and reduce the effort and cost of compliance activities. Our Compliance Services unit manages a growing portfolio of financial crime compliance services in the areas of Sanctions, KYC and CTF/AML.

SWIFT's Customer Security Programme, which launched in June 2016, is a dedicated initiative designed to reinforce and evolve the security of global banking, consolidating and building upon existing SWIFT and industry efforts. The programme will clearly define an operational and security baseline that customers must meet to protect the processing and handling of their SWIFT transactions.

SWIFT will also continue to enhance its own products and services to provide customers with additional protection and detection mechanisms, and in turn help customers to meet these baselines.

www.swift.com/complianceservices

57245 - January 2017