BAE SYSTEMS

Financial crime compliance professionals: mission impossible or tech-savvy super heroes?

BANKING INSIGHTS
FROM BAE SYSTEMS

The role of technology in overcoming challenges

In this Insight paper, Mariola Marzouk, Compliance Product Manager at BAE Systems, along with other experts from the BAE Systems Banking Insights team, investigates three key issues faced by financial crime compliance professionals – and asks what role technology can play in helping to overcome these challenges.

The chilling statistics reveal that around 1% of Suspicious Activity Reports raised by compliance teams result in conviction[1]. This leaves offenders to strike again, and leaves victims, against whom the offences have been committed, unappeased.

Unfortunately, this is just one of the issues making the role of the financial crime compliance professional a tough one.

For these hard-working experts, the job of safeguarding the financial ecosystem from criminal exploitation may sometimes seem like a mission impossible, particularly when the obstacles range from a lack of harmony across the international regulatory landscape, to jurisdictional level challenges between different legislations; all of which feed into internal operational hurdles.

Like all good protagonists, the odds are stacked against them. Below, we look at three hurdles in more detail, and ask what role technology can play in helping to overcome these challenges.

1 In 2018, Europol reported that the precision in detecting criminal fund transfer was only about 1% - *From suspicion to action – converting financial intelligence into greater operational impact (Financial Intelligence Group, Europol, 2018)*

The European Parliament has also recognised that just 1.1% of criminal profits get confiscated – *Criminal proceeds: making it easier to freeze and confiscate across the EU (European Parliament News, 2018)*

Issue #1: The false positive burden

Anti-Money Laundering compliance professionals are often overloaded with false positive alerts. However, despite approximately 90% of alerts being false,[2] each must still be investigated with speed and diligence.

A backlog is often frowned upon by the regulators, and can invite scrutiny that can ultimately lead to significant fines. But it's the reputational and remediation consequences of these fines that can have a greater and lasting impact on a financial institution.

For the compliance professionals themselves, the issue goes deeper than the threat of a fine. For many, the ability to spot and prevent instances of crime is crucial to their job satisfaction. And, in an environment where missing something or not investigating an alert quickly enough might mean instances of crime are slipping through the net, the regulator's judgement is even more meaningful.

> "Preventing criminals from enjoying the proceeds of financial crime, is what gets many compliance professionals up for work each day. So finding out that an alert is, for example, 'indicative of child exploitation' can hit you straight to the heart – especially if it's an alert that you simply haven't had time to investigate yet," explains Mariola Marzouk, Compliance Product Manager at BAE Systems.

Issue #2: The internal stereotype

Unfortunately, some operating within the financial services industry consider their compliance departments to be a cost centre, or even an obstacle to growth. This branding is no doubt a source of frustration for the compliance professionals themselves, because their role in fact has the potential to help organisations make good business decisions.

Although businesses are eager to secure sales and reduce friction in the buyer journey, in a world where sophisticated criminals look like legitimate businesses, having a compliance team that can sort the good from the bad is essential for de-risking new opportunities and enabling long-term business growth.

2 Based on a report issued by PwC, 90-95% of all alerts generated by transaction monitoring systems (TMS) are false positives – *From source to surveillance: the hidden risk in AML monitoring system optimisation (PWC, 2018)*

"As a compliance professional, you find yourself in the difficult position of balancing multiple and often contrasting priorities; protect the bank, protect society, and enable growth," says Marzouk.

Issue #3: Operating in a world of constraint

Many global regulators encourage banks to responsibly implement innovative approaches to meet their anti-money laundering compliance obligations. For example, customer monitoring – which involves sourcing more data to help in risk assessments – is one of many areas where technology could reduce the burden on compliance teams.

However, some banks find guidelines vague, and therefore lack the confidence to utilise the latest technological approaches available to them.

"Criminals, on the other hand, do not operate in the realm of such constraints. They are free to innovatively respond to any emerging opportunities, such as those that unfolded in early 2020 as a result of the coronavirus pandemic. What's more, there is no-one to scrutinise their decisions, and they are free to go where the intelligence leads them," says Gary Kalish, Senior Financial Crime Prevention Consultant at BAE Systems.

Can technology change the state of play?

Taking an intelligence-led approach can enable compliance teams to start to overcome these challenges, for several key reasons…

Freedom from the burden of repetitive or low value-add tasks: the use of intelligent technology to automate certain tasks can enable compliance professionals to work more creatively. Machine learning, for example, can improve detection rates and free up the workforce to be more proactive and inquisitive.

Furthermore, sophisticated and dynamic customer segmentation, based on peer group profiling with help of the advanced analytics techniques, is a prerequisite to an effective AML transaction monitoring solution. Automated alert triage capabilities can also ease the investigator's work burden and allow them to focus on the highest priority risks first.

With intelligent technology in place, compliance professionals can also be freed to upskill – for example by learning how to interrogate data sets and communicate complex ideas.

As Mark Rayner, Head of Consulting, Financial Services explains, "It is about building teams with a balance of skills that can dynamically complement each other and reveal intelligence behind data that can be effectively and efficiently operationalised.

"The banks that invest in technological change will have compliance teams that can achieve more, and be better equipped with skills for the digital age. This will allow them to use their roles to better serve society in the fight against crime."

Switching from reactionary alert work to holistic analysis: when compliance investigators are provided with simple to use, flexible, scalable and, above all, holistic technology, they can work in an intelligence-led manner to combat financial crime.

Advanced compliance solutions can enable teams to stop reactively responding to individual alerts, and instead focus on the holistic analysis of suspicious activities. Network analysis is a good example of this sort of intelligent technology – if seamlessly integrated with a holistic case management system, network analysis enables investigators to easily understand the relationship between various data points or entities.

> Marco Beranzoni, Financial Crime Consultant at BAE Systems, explains the value of understanding the relationship between entities: "Understanding a wider pattern in customer transactional behaviours can, for example, show how a small number of mules could actually be responsible for a disproportionately large number of child exploitation money laundering activities. Such intelligence is paramount to limiting the probability of such crimes passing through the bank."

Supporting the customer experience: regulators are advocating the use of advanced technology such as digital customer on-boarding and CDD risk scoring, to ensure customers can quickly access much needed banking products and services.

Being able to effectively risk score customers in real time during the on-boarding process not only helps banks weed out the bad, but it also provides exceptional customer service for those who are genuine in their intentions. After all, the best compliance measures prevent criminals from becoming customers in the first place.

The journey from mission impossible to tech-savvy super heroes

The mission of the compliance professional is only getting harder in the wake of the COVID-19 pandemic. As many customers adjust their financial behaviour, noise in data creates opportunities to hide criminal intent, and entrepreneurial criminals are set to take advantage of current circumstances.

> "The fact remains that fighting financial crime is a mammoth task. The numbers don't lie, trillions of dollars' worth of money laundering is still happening, and just the careless criminals get caught," says Marzouk.

Yet, banks are still required to meet their AML/CTF obligations, so working with reliable and expert technology partners can help compliance professionals to ensure that solid business decisions are prioritised in line with true business needs.

While the need for an intelligent-led approach to compliance is clear, the journey there isn't always simple - it requires a shift from tactical volume, value and velocity monitoring for suspicious activities, to a more strategic and subjective assessment of threats, vulnerabilities and consequences.

Ultimately, working with a technology partner that can guide them on their journey, is crucial for compliance teams that wish to adopt a new approach.

At BAE Systems we continue to invest in our technology and offer a wide range of services with full awareness of the challenges faced by the industry. We support the financial services sector in defending itself, reducing risk in the connected world, complying with regulations and transforming operations.

Our technology is already helping compliance teams around the world switch from working on seemingly impossible missions, to become tech-savvy financial crime fighters. If you'd like to find out more about our experiences, please get in touch.

Explore our range of resources and further reading

In the meantime, we've collected some further reading about cybersecurity (and developing the next generation of cybersecurity specialists) below. Explore the materials and share them with your networks.

- Explore: compliance solutions that reduce your risk
- Read: The banker in 2050 – the role of the human in fighting financial crime
- Discover: Banking Insights content straight from the experts
- Contact: Mariola Marzouk now

About Mariola Marzouk, CAMS, CITF

Compliance Product Manager at BAE Systems

Mariola manages the BAE Systems Compliance product line and has years of experience as an anti-financial crime strategist. She holds a Masters in Forensic Accounting and is currently working towards a Doctorate in Criminal Justice. Along the way, Mariola also holds an ACAMS certification, is certified in International Trade Finance by the London Institute of Banking and Finance and is certified in Corporate Finance by the Chartered Institute of Securities and Investments.

Aside from managing the development and maintenance of banking compliance products for BAE Systems, Mariola is also currently researching Trade Based Money Laundering problems and potential reforms.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
E: learn@baesystems.com | W: baesystems.com/bankinginsights
linkedin.com/company/baesystemsai
twitter.com/baesystems_ai