BAE SYSTEMS

# Real-Time Transaction Monitoring: Time to get real?

# Executive summary

**Gary Kalish**
Senior Financial
Crime Prevention
Consultant at
BAE Systems

**Stephen Blackburn**
Senior Financial
Crime Consultant at
BAE Systems

Disruption continues to reshape the financial services industry. Time-proven products and services have been rendered obsolete in the blink of an eye, rewriting the banking landscape and leaving it created with new challenges.

Online banking and faster payments have been happily embraced by customers – good and bad. Money launderers, just like fraudsters, see change as opportunity. But while fraud checks and sanctions screening are already happening in real time, transaction monitoring for Anti Money Laundering is looked upon as the next logical solution to take its place in the Real-Time armoury.

# Real-Time Transaction Monitoring – why now?

In the past, institutions' anti-money laundering (AML) activity primarily involved the batch-sorting of transactions at the end of each working day. This approach was based on looking at a customer's behavior against known money laundering typologies. Now, though, 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 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.

Brian Dilley, Group Director of Fraud and Financial Crime Prevention for Lloyds Banking Group, points to the fact that the overlap of fraud and financial crime is itself catalyzing change:

"The scenario where the proceeds are gone before you have actually identified something and the fraudsters get away with the money is no longer sustainable," he says. "But the question is, what subset of criminal behavior should we be aiming to detect and prevent by stopping transactions in real-time? With fraud in retail banking, the argument is clear, however when you look at something like human trafficking, stopping an associated financial transaction doesn't necessarily stop the crime from taking place. In this case a post-event, intelligence-led approach to prevention is actually more effective."

There are also several other factors to consider – not least the enduring impact of technology.

Technology

Regulatory

Silo-Busting

# Technology

Such ideas are clearly suggestions that can be tailored to the individual challenges facing each insurer, large or small. But their adoption can make all the difference between preventing a catastrophic internal attack and achieving secure internal data and systems.

Technology is rapidly changing the way organizations deliver products and services to customers. But with these advances and increasing connectivity comes greater risk.

Matt Saint, AXA's Group Anti Money Laundering Officer, points out that technology's impact has been clear to see. "In the early years, the technology was pretty static but then there were developments, particularly relating to client identification and the electronic identification of customers," he says. "Subsequently you're starting to get more into the automation of activity monitoring and then today we see further developments of digital biometric client identification."

Biometric identification is something that Lloyds Group has prioritized. "A lot of the success we're having is thanks to behavioral monitoring which is about device IDs and indicators of unauthorized access," says Brian Dilley.

"We do this in both real-time and post-event but my view is we need to move away from purely monitoring transactions and into monitoring of behavioral characteristics. This involves looking for indicators in the way people log on and use their device that show they are up to no good. It's perfectly legitimate for an application to be made by one device for more than one name but once you go past a certain number it's highly unlikely that those are legitimate. It's not about merely complying with the regulations but more about reducing harm. We're deliberately called 'Fraud and Financial Crime *Prevention*' rather than 'Fraud and Financial Crime *Compliance*' which is a deliberate statement because we're not just about complying with regulations, we're about *preventing* fraud and financial crime."

# Regulatory

As you'd expect, preventing money laundering and terrorist financing are twin priorities for governments and regulatory bodies worldwide. And when the increasing prevalence of cross-border data exchange is twinned with customers' justifiably high expectations around data security, it should come as little surprise that compliance legislation has become more complex and wide-ranging.

For example, in some parts of the world insurers may be compared to banks, and regulators may subsequently expect them to adopt similar standards of control. Regulators are also insisting on more detailed Suspicious Activity Reports from institutions. If financial institutions fail to comply with such regulatory obligations they risk multi-billion dollar enforcement actions.

It is important to note that regulators today do not always have a consistent approach around the world, for a variety of reasons as they move at different paces in different places. Countries bracing for an evaluation from the Financial Action Task Force may seek to ratchet up their levels of compliance prior to the arrival of the inspection team but take a step back, and you can see that some regulators adopt a light touch, whereas others are more aggressive.

Although the regulators in some of the smaller geographies tend to be focused primarily on domestic issues, this is not always the case. There are a number of these geographies across the world that pride themselves on a high level of compliance that mirrors regimes in place in Europe and North America.

# Silo-Busting

AML activities – both non-real-time and real-time – help make information more readily available across an organization. This is partially helpful in breaking down the silos that can all too frequently occur between those working in AML and their colleagues in fraud prevention. AML systems draw from a wide range of transaction types and sources and these can potentially provide the fraud detection teams with valuable intelligence – especially if this can be provided in a timely manner.

## Real Challenges for Real-Time

Although there are significant forces lining up to support its wider deployment, Real-Time Transaction Monitoring for AML is no panacea.

For example, it lacks the ability of batch processing to identify patterns that may not otherwise be apparent. With real-time, if you are looking for things as they happen you can sometimes get alerts for payments that don't go through – due to credit limits being hit, for example. One danger is that it produces a bigger haystack for investigators to hunt through – something that Lloyds' Brian Dilley is well aware of: "I don't think full-scale Real-Time Transaction Monitoring is practical given the volumes of suspicious activity that occur and the fact you would have to stop so many transactions for the false positives as well," he says.

There are also technology issues to address. Rating a cash transaction in real-time, when some branches are probably only posting the transaction at the end of the day, is far from straightforward. Real-Time Transaction Monitoring requires a more complicated architecture. Relevant data has to be sourced and delivered to the monitoring system in real-time; determining AML behaviors often relies on the sequencing of events: How can the sequence be preserved across multiple data feeds? Stronger high availability and failover requirements are necessary.

Then there are challenges around implementation. If there is a demand for real-time alerts, an organization needs to have the right people in place to deal with them. Brian Dilley adds that this is a serious challenge.

"If you were to do Real-Time Transaction Monitoring for everything you look for in post-event transaction monitoring you would grind the payments system to a halt and need thousands and thousands of people because you'd be stopping so many transactions. So the question really is what are the things that are most important to intervene on and stop happening? Fraud is right up there because you're talking about protecting your customers, and customers of other banks, from being defrauded and stopping the crime from happening."

Implementation is also an issue that AXA's Matt Saint is well aware of. "You need to be mindful about how diverse our businesses are," he points out. "Because we're different from a global bank – we have a different mix of corporate, B-B-C and retail businesses – we cannot always have a one size fits all; it just doesn't work. What we are aiming to do is to build a central core of technology that is applicable for the majority of the business and then there may be some tweaks around the edges."

# Five top challenges for Real-Time Transaction Monitoring

1

## Aligning business strategy

In the past it would take days to onboard customers and to make payments. The pressure now is to align strategy with operational reality.

2

## Just do IT

The IT architecture required to enable Real-Time Transaction Monitoring work effectively is becoming more complex. Many large organizations have to cope with legacy systems and deploying the right architecture to do the right check at the right time is hardly straightforward.

3

## Banking confusion

Regulators, rightly or wrongly, often expect insurers to banking standards. This places pressure on insurers to adopt stricter, more resource-intensive, regimes than have been in place in the past.

4

## No one size fits all

As AML is a global risk there are differing approaches taken by nation states on their respective response.

5

## What about the output?

Real-Time is one thing but managing its output is quite another. Organizations have to be able to deal with what real-time checks produce and have the systems and operations in place to deal with it.

# Over the horizon

The push for Real-Time Transaction Monitoring has not appeared overnight. Rather, it has emerged as a result of myriad different factors and developments. Even now, it has yet to meet with universal acceptance amongst financial services companies and law enforcement agencies.

But it's important to note that these things take time. Technology needs to be rolled out, staff need to be trained, and organizations require the necessary resources and confidence in order to fully augment their AML arsenal.

It seems likely that Real-Time Transaction Monitoring will continue to gain traction in the months and years to come. Digital technology will continue to evolve; financial firms will be under ever more pressure to submit better reports; the number of false alerts will continue to rise and criminals will always seek new ways to hide their illicit gains.

A decade hence, we can say with some certainty that the AML environment will look very different to that of today. Although there will still be traditional AML activities – possibly driven by machine learning – monitoring checks will be likely happening in real-time, as will closer interaction with fraud detection teams.

As a result, those organizations which start to invest now in forward looking AML technologies will not only reap competitive advantage, but also be better placed to prevent money launderers from successfully penetrating their defenses – both now and in the months and years to come.

## Profiles

# Gary Kalish

### Senior Financial Crime Prevention Consultant at BAE Systems

Gary Kalish works within the Financial Services market including retail, commercial and investment banking, applying his knowledge and experience to support organizations mitigate their risks from serious and organized crime in an increasingly complex regulatory landscape.

Gary holds a Masters in Security and Risk Management from the University of Leicester with over 16 years of experience in financial crime risk management. During this time he has worked in the financial and public sector on both a local and international level with expertise in identification, analysis and mitigation of risks including money laundering, terrorist financing, fraud and market abuse / misconduct.

# Stephen Blackburn

### Senior Financial Crime Consultant at BAE Systems

Stephen Blackburn works with Financial Institutions in retail, commercial and investment banking, applying his knowledge of BAE Systems Applied Intelligence solutions together with experience in the banking business to help tackle the challenge of remaining compliant in an increasingly complex regulatory landscape.

Stephen is a Certified Anti Money Laundering Specialist (CAMS) with a experience in AML transaction monitoring. Over the last 20 years he has also been involved in Sanctions and PEP screening, payment filtering, Know Your Customer (KYC) and Customer Due Diligence (CDD).

# How we can help

### Rising to the technological challenge

Real Time AML demands a more complicated architecture than what has worked in the past. We possess the domain knowledge and technology solutions that combine speed, intelligence and efficiency to detect and prevent financial crime.

### Stay ahead of regulatory requirements

Failure to comply with sweeping and evolving regulations puts financial institutions at significant risk of reputational damage, substantial fines, and potential loss of their banking licence. We help organizations navigate increasingly complex compliance legislation while also driving efficiency, preventing more crime and nurturing business growth.

### See the bigger picture

Our world today is highly complex and interconnected. Advances in technology mean that people, money, and merchandise move around the globe faster than ever before. We look at suspicious behaviors across various product lines, departments and channels in order to build a holistic view of an entity and strengthen its defenses.

For more information go to: www.baesystems.com/bankininsights

## Contact us

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

**Victim of a cyber attack? Contact our emergency response team on:**

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

linkedin.com/company/baesystemsai   twitter.com/baesystems_ai

BAE SYSTEMS