NICE · ACTIMIZE

A risk-based approach to AML and financial crime risk in Asia-Pacific

Financial institutions across Asia-Pacific are grappling with fast-changing risks and digital transformation in their efforts against money launderers and financial criminals. *Risk.net* hosted a webinar in association with NICE Actimize to discuss the changing situation

The year has not yet come to a close, but it already qualifies as living in interesting times. The Covid-19 pandemic and its consequences have provided Asia-Pacific's banks' anti-money laundering (AML) and financial crime teams with unprecedented challenges, adding to the existing mesh of cyber crime risks, trade tensions and pressures of regulatory scrutiny faced by risk managers.

For financial criminals, on the other hand, the fast-changing environment of the pandemic has created conditions they can exploit in their unending efforts to scam and defraud, and wash the proceeds of criminal enterprise within the financial system.

Taking a risk-based approach to fighting financial crime provides certain advantages in its agility and flexibility. In support of a risk-based approach, banks are deploying more advanced weapons to boost their capabilities to detect crime, including applying artificial intelligence (AI) and machine learning to analyse growing volumes of data.

However, many of these technology projects are still in the early stages of model development, testing, validation and implementation, with some significant barriers still to be overcome before they become part of the 'new normal'.

"The cost of managing AML programmes is not decreasing: adoption of AI technologies has been limited, and effort and labour costs remain high," said Matthew Field, Asia-Pacific market director, AML at NICE Actimize.

Key factors

Risk managers are accustomed to tough choices. An audience poll question during the webinar discussion asked: "What are the key factors to consider when implementing a more active risk-based approach to financial crime management?"

The options for response were: deploy advanced technology such as AI and machine learning to monitor customers' risks; develop detailed money laundering risk assessment on all the company's products; proactively monitor every transaction in real-time; and conduct stringent, truthful and accurate customer checks.

The results to this question were split, perhaps unsurprisingly, given the relevance of each of the options and the leeway for different approaches that a risk-based approach provides. However, the first two options came out strongest: using advanced technology, and developing detailed risk assessments for products.

Much of the industry's innovation is still in the proof-of-concept stage, according to Field. "If you look at how AI and machine learning can help a risk-based approach you have got to focus on the things that make detection and decision-making better quality and more efficient," he said. Much of the work remains to be done, but there is a spirit of optimism about the road ahead.

"There's a lot of innovation happening and that's exciting, but I think we are still a number of years away from driving more effective financial crime outcomes," said Nick Davison, partner, financial crime unit, South-east Asia consulting at PwC.

Matthew Field, NICE Actimize

Beyond tick-box

Banks are increasingly thinking beyond the tick-box compliance exercises that were common a generation ago. This is partly as a result of the actions of legislators and regulators, but also greater enthusiasm within institutions about the potential improvements in efficiency and effectiveness that can be brought about by harnessing AI and machine learning technologies.

A good example of this is in institutions making greater use of consortiums for data sharing, adding these to traditional internal sources, Field noted. Once harnessed, those new data inputs put greater onus on using technology to analyse them.

"The financial crime detection and prevention market is looking towards public or private cloud AI and machine learning services because of lower costs and higher speed to start-up, allowing for much faster benefits from the models run," he said.

Many financial institutions are also embarked on "de-risking exercises", Field explained, with options for how to achieve this. "They're asking: 'If this is a highly risky product or channel, do I exit from it? Or else, how do I put stronger risk controls around it?" Field added.

For banks adopting a risk-based approach, this means a high degree of flexibility. It does not equate to prescribing one-size-fits-all financial crime requirements, Field suggested. This is particularly the case for AML, which focuses on how to detect suspicious activity, rather than fraud, which is focused on absolute prevention.

"We are seeing different strategies adopted between fraud and AML," Field said. "In AML there is more acceptance of risk, which can then be managed, mitigated or transferred, whereas in fraud the aim is to prevent risk occurring outright. Of course, it is important to have the ability to prove to the regulator, the board, auditors and other stakeholders that you are managing these risks properly, and this is a challenge in itself."

However, when considering how AI and machine learning technologies can support a risk-based approach, it is important to consider solutions that can have applications beyond one facet of financial crime fighting, including fraud prevention, AML, counterterrorist financing or sanctions regimes.

"AI and machine learning can help improve fighting financial crime, and are chipping away at aspects of sanctions, particularly in the screening space," said Maggie Qiu, Greater China and North Asia regional head of sanctions, financial crime compliance unit at Standard Chartered. "This is a continuing top risk for many of the clients of my firm, as well as top priority for our own financial crime compliance," she added.

Pandemic shifts

Sudden change such as the Covid-19 pandemic and its economic consequences have created major challenges for banks' financial crime teams. The pandemic has turned old assumptions on their head almost overnight.

Companies and customers working remotely, relying on public internet services more than ever before, has opened all sorts of vulnerabilities that cyber and other criminals have been seeking to exploit. Another audience poll question during the debate, on banks' preparedness to tackle an increase in fraudulent activity, brought back mixed results. Risk managers at some institutions stated themselves well prepared; others admitted to a lack of confidence.

This is also unsurprising, because the pandemic has created some unusual challenges for financial institutions, particularly international banks. System performance, remote working capacity, operations and planning are all under pressure, according to Qiu.

"Some banks are better prepared than others," she said. "We have weekly control check-ups on how the staff and the systems are performing. Senior managers monitor productivity and the operational status daily. I see an acceleration of adopting technology in the current situation and part of a bigger trend, particularly AI, robotic automation and machine learning, for transaction monitoring and screening."

Field highlighted the research undertaken by NICE Actimize to gauge the reactions at least 30 international financial clients as the Covid-19 pandemic unfolded. "A lot of them said they wished that they had more automation in place, so we would expect digital transformation with robotics to continue and to accelerate as a result of Covid-19," he said.

"Data aggregation as well as automation looked like an achievable opportunity. Some of our clients were saying you need to be better able to aggregate data into one analyst view, so you can assess the risk easily and with more confidence," continued Field.

Financial services organisations' customer behaviours changed dramatically during the lockdown period, and will likely continue to change into the new normal after the pandemic. "We have a situation where almost everybody is behaving in a very different way to how they were two or three months ago," said Davison.

Field continued, offering some examples of changing customer behaviours: "There was a rise in the volume of internet and mobile phone transfers. Different transaction amounts, out of normal transaction behaviour, were being transferred, and banks were struggling how to quickly react to change their thresholds and to simulate the impact of all of this."

All of this has had serious consequences for the models banks have in place to detect suspicious activity. "These are based on the expected behaviours of their customers and monitoring for anything out of the ordinary," Davison said. "The number of 'suspicious activity' alerts for our clients has been absolutely enormous in recent months, because everybody is acting outside of expected parameters."

In the new situation, a customer showing 'business as usual' behaviour suddenly looks suspicious amid pandemic conditions, Field warned, playing havoc with models for customer risk ratings unless they are adjusted accordingly.

"If you have businesses that are basically shut down over this period but are continuing the same sort of transaction behaviour that you saw previously, you have to ask what is going on," Field said.

"This is the area we think there is real danger. It is quite a unique challenge that anybody continuing business as usual represents a red flag as to why that is and what is really going on with those clients," he said.

The scale and speed of change means scheduled risk reviews for products and high-risk customers will also need to move towards real-time in future, Field reflected, putting further onus on the use of technology to speed up processes.

"The days of high-risk customers having periodic reviews every six months may be not effective," he said. "They will need to have continuous risk assessment. That is going to be an interesting process to manage going forward."

Criminals have meanwhile been busily innovating new scams during the pandemic, meaning banks have still more new types of suspicious activity to look for. "In Asia we've seen a lot of scams and fraudulent activity related to face masks, protective clothing and medical equipment," said Qiu. "We are also doing some interesting public engagement work related to money scam emails."

The change in criminal behaviour is a consequence of criminals facing challenges of their own during Covid-19. The pandemic has removed some opportunities from them as well as creating new ones.

"We have seen significant reductions in the amount of cash transactions, making it difficult for criminals wanting to launder cash," said Michael Clarson, Asia-Pacific regional head, global investigations unit (GIU) at Citibank. "However, cross-border wires have increased significantly, providing plenty of opportunity to commingle and utilise money laundering techniques."

Because Asia is such a huge region with so many borders, the variation in local rules and regulatory differences during the pandemic can mean customer behaviour and suspicious behaviour can differ substantially from one country to the next.

"We have recognised changes in behaviour within each jurisdiction based on the country's rules and restrictions, for example the Movement Control Order in Malaysia," said Clarson. "Other restrictions in other jurisdictions in terms of people's movement will affect behaviour as well. We have preloaded that behaviour into expectations of our transaction monitoring. The alerts have changed, and we see that if we are not agile enough we get an increase in alerts based on scenarios not been adapted for this behaviour."

Field described another example of suspicious activity during the pandemic, involving an organisation concerned with movement of funds through a jurisdiction and industries that were previously not thought of as high-risk.

"It is interesting that the launderers have moved into what you might call typically trusted segments," he said. "The low-risk segments being used had received a number of government handouts and benefits, so looks like unusual behaviour but with mitigating circumstances. The feeling was that the bad actors had deliberately decided to move into what they knew we deemed a low-risk industry segment where more unusual transaction may occur due to the handouts."

Onboarding new customers represents a risk exacerbated during the extraordinary new normal of the Covid-19 pandemic. "That is a vulnerability when you try to onboard new clients in a completely restricted environment, and criminals are taking advantage of that by establishing new accounts," Clarson added.

Digital onboarding risks have represented a challenge for banks to continue welcoming new customers. They will also need to learn lessons for the longer term, Field argued, to continue to verify customers are legitimate, law-abiding, and that they are who they say they are.

"There has been such a rush for digital identification for onboarding purposes," said Field. "Once the pressure is relieved after Covid-19, banks are going to have to consider how they continue to do this in the longer term in a responsible and risk-based manner."

New ways of working

Digital transformation offers the potential to increase the effectiveness and efficiency of processes for countering financial crime – representing two different but closely interrelated benefits.

Improving the efficiency of existing processes and operations is an immediate focus for Davison's team, he emphasised, trying to improve outcomes by enabling analysts performing financial crime detection operations to focus more on actual financial crime risk, rather than process and information gathering.

"Examples include negative news screening, where we have AI that can automatically disposition 70% of the alerts that are generated, saving analysts large amounts of time. This allows them to hone in on the risks that are presented, rather than review page after page of false positives, which is what they're often presented with at the moment," said Davison.

Predictive or automated quality control (QC) is another example in the same vein, he suggested. "We know quality is vital for all of our financial crime processes, and using data and machine learning to drill down into analysts' past performance, for the types of know-your-customer cases they're looking at, enables us to predict where they are likely to make mistakes," he continued.

This analysis helps to drive efficiency as we can use it to "either green-light certain analysts on a particular type of case where on a risk basis we can accept this analyst is very unlikely to make a mistake. Or it can be used to direct QC efforts to focus on particular areas where the likelihood of an error has been shown to be higher, rather than the whole case," Davison added.

Field pointed to segmentation and machine learning-driven advanced segmentation as some of the low-hanging fruit being grasped by banks, representing a more proactive way to catch dirty money being moved. In some cases this is replacing 10-year-old screening rules that are increasingly wrong or irrelevant.

"A machine can help us find the relationships to other entities that we can't easily see based on the old rules. That is one area where we are seeing AI and machine learning applied to a risk-based approach, such as in the efforts to detect anomalies in transactions, highlighted by Nick [Davison]," he said.

One example of a risk-based approach is Citibank's GIU team, which provides an external view on the typical financial crime lifecycle elements of transaction monitoring, prevention, detection, reporting and response.

"The GIU sits outside of that linear process, and we are nimble and agile in terms of how we can direct our resources, having spent many years getting access to data across multiple jurisdictions," said Clarson. "It is that supplementary specialist activity I think that adds value, particularly in environments like we are in at the moment with Covid-19."

Looking for partnerships to make better use of external data, such as data consortiums mentioned previously, is one area shifting from old to new. This is something the GIU has been busy with, Clarson explained, particularly public-private partnerships and liaising with law enforcement, in the US, across Asia-Pacific and globally. "We're able not only to assess requirements within a single jurisdiction, but to identify risk across multiple jurisdictions, and ensure that there is an enterprise wide approach to customers, and groups of customers, in terms of how we manage risks," he said.

"As a specialist investigations unit, adopting a risk-based approach, we collect intelligence and data internally and a large amount externally, and that is in structured elements, and this drives a significant amount of our work," he added.

Adding machine learning to the mix is about both driving efficiency and increasing effectiveness, emphasised Clarson, who wants to use digital transformation to crunch ever greater data volumes more quickly, while taking care that technology costs never outweigh the savings provided.

"Collecting external unstructured data and quickly coming to a clear position on its assessment is important," he said. "We can employ intelligent people to focus on identifying the highest risks, managing and mitigating them."

Most banks share a focus on efficiency and keenness to keep costs manageable. Transaction monitoring and screening processes are the usual starting points for embracing AI and machine learning, Qiu noted. Many functions previously undertaken by a junior analyst, she suggested, are now considered potentially replaceable by machine or robotic automatic process.

"The process is one of retrieving and mapping information internally across different bank systems and platforms, from the public domain or from external lenders, can be unstructured or structured, combining data, analytical segmentation and so on," she said.

Governance risks should remain front of mind when considering adopting advanced technology, such as machine learning tools. Models need to work as intended once the human touch has been all but removed, with effective oversight to ensure that continues. Roll-out will take time and testing.

"For large banks there is concern before we adopt any machine learning or any other AI technology," said Qiu. "Data quality, system performance, data privacy, model validation – all require governance and dedicated expertise, and if any of those go wrong it will create more regulatory risks for us."

Communicating with the regulator about the introduction of AI into models marks another challenge, Qiu highlighted, to ensure they remain comfortable with changes to the risk-based approach.

Field added: "You have got to be able, from a governance perspective, to prove through the right documentation around the models that the sample is representative to produce the necessary information that you are going to use to figure out whether the non-alerted activity was suspicious or not."

Davison stressed that any potential for "big black-box models" is some way away, and that the governance and regulatory challenges are manageable for the ways in which AI is currently in use or for which it is being tested.

"Given how we now use AI and machine learning technology to drive efficiency and help analysts focus on financial crime risk, it is relatively straightforward to govern the technology through regular testing of models to make sure that they are operating as intended," he said.

The primary focus is still on increasing efficiency, without negatively impacting effectiveness, Qui emphasised, rather than using more advanced machine learning to begin in a more profound shift towards greater effectiveness further down the road.

"This is a big trend, but it's still the early stages to leverage AI at the next level, and it will take some more time to unlock the potential," she said. "Most projects are in the proof-of-concept stages of AI and machine learning, with the aim of to reduce the time and resources spent gathering information, whether internally and externally."

>> Listen to the full webinar, *Adopting a risk-based approach to AML and financial crime management*, at *www.risk.net/7550716*

The panellists were speaking in a personal capacity. The views expressed by the panel do not necessarily reflect or represent the views of their respective institutions.

Fighting Financial crime.
It's what we do.

NICE
ACTIMIZE

X-Sight
DataIQ

Transforming Data into Actionable Insights

Make smarter and faster decisions throughout the customer lifecycle with the power of data and analytics.

START SMART
Validate and enrich customer data

STAY INFORMED
Accurate customer intelligence

COMPLY CONFIDENTLY
Improved risk ratings

www.niceactimize.com/data-intelligence | info@niceactimize.com