NICE · ACTIMIZE

Deploying agile analytics in the fight against fraud

Financial firms are under pressure to tackle the widespread problem of financial fraud. As the speed, scale and sophistication of fraudulent activity grows, a panel of financial crime experts reveal how firms can develop an agile analytics capability to help mitigate the threat

Building a resilient fraud risk management framework is a complex challenge for today's financial firms. It requires analytical tools, skills and capabilities to enable appropriate protection against constantly evolving and malicious fraud attacks.

With this in mind, *Risk.net* convened a webinar to examine how practitioners are approaching the use of analytics in fraud detection programmes, and to offer insight around best practice and tools being deployed by banks and others in the industry.

Among the discussion points were the use of agile analytics in fighting rapidly shifting fraud attacks, the merits of combining vendor-based and 'homegrown' analytics, and the opportunities in artificial intelligence (AI) and machine learning.

THE PANEL

Damian Matich, Global head of fraud and analytics, NICE Actimize
Henry Jiang, Director of fraud, analytics and strategy for global banking and markets, Bank of America Merrill Lynch
Michael Schidlow, Former head of financial crime compliance and emerging risk audit development, HSBC*
Moderator: John Anderson, contributing editor, *Risk.net*

**Michael Schidlow has since left HSBC and is now a financial crime compliance advisory and training consultant*

The need for agile

Agile analytics has become an essential weapon in the fight against fraud. As the scale and sophistication of criminal activity has grown, so has the need for smarter, faster solutions to track and analyse activity as part of a more proactive risk management framework.

Until the 1990s, traditional rules-based systems had been quite effective in defending financial institutions against fraud, according to Damian Matich, global head of fraud and analytics at NICE Actimize. But the advent of the internet and the explosion of customer digital channels and products opened up more opportunities for criminals.

"Fraud started to morph into multi-faceted, multichannel attacks," said Matich. "Agile analytics is a response to the increasing sophistication of fraudsters and fraud syndicates in attacking financial institutions."

The speed of that response is a key concern for Henry Jiang, director of fraud, analytics and strategy for global banking and markets at Bank of America Merrill Lynch. "The fraudsters are operating at a global level," he said. "It's an industry for them. They roll out new [fraud schemes] very quickly on a large scale… so we have to come up with our new prevention models in a short time period."

Michael Schidlow, former head of financial crime compliance and emerging risk audit development at HSBC, has no illusions about the difficulty of the challenge. Quoting an industry colleague, he likened financial crime risk management to "policing a highway with no speed limit, trying to chase Ferraris on a bicycle".

Schidlow pointed to a highly organised tax fraud case from his time in investigations as an example of the increasing sophistication of criminal activity, and where agile analytics is starting to make a difference.

In this instance – a stolen identity refund fraud – the fraudsters had even hosted some kind of online workshop to explain and disseminate the scam's modus operandi, Schidlow said. The scheme involved taking synthetic and stolen identities to file huge numbers of false income tax returns, generating hundreds of electronic tax refunds.

So how can agile analytics help? Rather than a series of rules-based controls that banks might use to look for basic deviations from a profile, Schidlow said a more sophisticated analysis of specific language and typology will help weed out large numbers of unstructured false positives. This saves analysts time and effort and ensures the key information is carried through to a suspicious activity report.

The AI opportunity

Some firms are also exploring the potential of AI and machine learning in the fight against fraud. According to Matich, current initiatives include supervised and unsupervised techniques – running cross-channel analytics, detecting anomalies on transaction streams and providing industry views – but firms are only just beginning to tap into the potential.

A key factor determining the success of these new technologies is the quality and volume of data available, particularly in low-volume channels.

Having encountered numerous examples of fragmented or siloed data that hampered the effectiveness of more basic processes, Schidlow is passionate about the need for risk-sensitive data validation.

"If you're not doing it right for transaction monitoring, if you're not doing it right for receivables finance, you're not going to get it right with AI," he said. "Financial crime risk-sensitive data should be pushed up to the front of the data validation process."

Modelling techniques such as proxy sampling can be useful in mapping fraudulent behaviour patterns between portfolios, noted Jiang, but up to 80% of development time should be spent in data sourcing, cleaning and exploration.

"To be agile you need to simplify," Jiang said. "We have to collaborate with our peer groups to simplify our process. If you can streamline end-to-end – [including] cyber security, application security, fraud, financial crime… and data scientists – it helps to increase the number of data sources available. We have to build that enterprise-centric view with the data accessible across many different business lines."

Damian Matich, NICE Actimize

Getting organised

One useful lesson in developing an effective agile approach comes from the criminals themselves.

"The fraudsters don't work in business silos. They work as highly organised, effective teams and attack vectors that are highly successful," Matich said. "So we need to restructure, reorganise as teams, bringing [business, analytics, technology and data people] together with an understanding of each other's challenges."

At a global financial enterprise, this means co-ordinating teams, integrating and automating processes on a continuous basis.

"We optimise our workforce with dynamic adaptability [to] the change in the fraud environment globally," Jiang explained. "We define future fraud and associated capabilities and requirements and then we develop fraud hubs, so we can rapidly deploy our versatile resources. [We] shape end-to-end fraud management for those peak demands, quickly evolving the fraud patterns with global capacity and local expertise."

Schidlow believes this sort of agility can only happen where a strong governance framework is in place and roles and responsibilities are clearly understood.

"There are various stakeholders who are risk stewards for some of these components… but they don't necessarily need to be advised of the underlying guts of a structured query language query," he said. "They want to know the outcomes."

Forward planning

To stay one step ahead of the criminals and maintain an agile approach, firms must develop the tactical bandwidth and resources for dealing with current in-flight fraud cases while evolving a horizon-scanning, preventative strategy to navigate the changing fraud landscape.

Noting that the needs of a global bank will be very different to smaller, regional entities from his time in investigations, Schidlow recommends having two fraud intelligence teams examining the current caseload through separate lenses – one tactical and one strategic.

"If [an incident] is unique then it requires a tactical response," he said. "If it is more [systematic] then that needs to go to exception reporting… to be reviewed by a governance committee to decide whether [current] resources are sufficient. The strategic team would take the management information from [cases such as] card compromise or business email compromise and turn it into forward-looking strategies.

"Whether it's investigative staff, whether it's analytics or some other remediation… that goes back to whether or not you're tracking management information and exception reporting around those type of incidents."

Build or buy?

A further consideration for banks moving to an agile environment for fraud analytics is whether to develop capabilities in-house or adopt a third-party vendor solution.

Highlighting the trend towards agile open analytics, with the degree of commoditisation resulting from open-source technology, Matich noted that either option is possible, or a combination of the two.

"We're agnostic… about the analytics NICE Actimize clients use," he said. "We are exposing that core tech – in terms of the models we develop, the model validation and governance processes. "Secondly, we provide those tools to our clients to develop their own, using their own expertise to develop their own models on their data that we hold for them. Finally, they have the choice to use other third-party tools and export the results into our environment. We see our role as [providing] an execution platform and industry expert advice."

Matich believes this cross-industry insight on best practice is a strong draw for clients, coupled with vendors' commercial imperative, which helps to focus activity on business outcomes.

Jiang echoed this sentiment, noting that some vendors have been working with AI and machine learning applications for many decades and using consortium data to develop models. "Those kinds of off-the-shelf solutions combined with the best practice… solution providers [can offer] when they're working with many different clients globally and that knowledge of intellectual property is very valuable to us," he added.

Shared insight

While consensus is building around the need for greater industry co-operation in the fight against fraud, knowledge sharing and interfirm co-operation have so far tended to happen on more of an *ad hoc* footing.

"A lot of what I have seen has been very informal," said Schidlow. "There will be forums, there will be committees, there will be industry trade groups and their subchapters that will meet and discuss some of these issues, or at least they're designed to do that. [But] due to time constraints, due to subject matter interest... the messaging might not necessarily resonate.

"In the US, we have the 314 mechanism for information-sharing, which should be leveraged under the US Patriot Act when we are following the money. At the same time, the practical implication is that often there is [just] a phone call between people who know each other or… between people whose names have surreptitiously wound up on a spreadsheet that is passed around among investigators. The challenge is that there is not an audit trail if there's an informal information-sharing mechanism."

The information base is rapidly expanding, according to Jiang, with his firm collecting both financial and non-financial data from a range of internal and external sources, improving detection with real-time data and lookback profiling to segment populations and refresh models.

Matich is enthusiastic about the need for a more formal industry approach and the development of ActimizeWatch, his firm's cloud-based anti-money laundering and fraud analytics and information-sharing facility.

"We very much subscribe to the industry view," he said. "We're in a united fight against the fraudsters. The whole strategy of NICE Actimize is to provide an industry platform for information exchange, to have de facto consortium views of risk and then to bring that insight into our specific client analytic outputs."

>> Watch the full webinar, *Fighting rapidly shifting fraud attacks – Agile analytics in fraud risk management*, at *www.risk.net/6611196*

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.