Data analytics and automation part of the tool kit for a safer banking environment

Jan 8, 2019
The Business Times
https://www.businesstimes.com.sg/opinion/data-analytics-and-automation-part-of-the-tool-kit-for-a-safer-banking-environment

VENKY SRINIVASAN

Up to US$3t a year is laundered globally, and a banking regulation is created every 12 minutes. It's why more sophisticated and agile tools are needed to fight the scourge.

THE banking industry has had its share of money-laundering and fraud schemes over the last five years. These issues have become significant enough for banks to start investing heavily in some form of defence.

Yes, there are strict Know Your Customer (KYC) processes in place to verify the identity of customers and curtail some of the risks, and regulators have stepped up their requirements to ensure the country risk elements are dealt with efficiently - but these methods are not able to detect all financial crime, which evolves on a day-to-day basis.

Incidents of client data (financial and personal) being hacked and held for ransom are commonplace now. Money laundering activities revolving around the sale of drugs, weapons and terrorist financing have also picked up over the years. Financial fraud, which has always been the mainstay of technology-savvy criminals, has also increased markedly across geographies. There are numerous cases of online scammers and swindlers in the news every day.

There are times when the perpetrators come from within the bank, as in cases of unauthorised trades and bribery and corruption. Banks have the dual tasks of not only keeping external parties out of their systems, but also keeping an eye on internal processes and trading activities, in alignment with regulatory requirements.

According to the Monetary Authority of Singapore (MAS), on criminal conviction, S$16.8 million in financial penalties and compositions and S$698,000 in civil penalties were meted out between July 1, 2017 and Dec 31, 2018. Add to this the 19 prohibition orders, 37 reprimands, 223 warnings and 444 supervisory reminders issued over that period.

Despite the penalties handed out, the business, technology and regulatory landscape - as well as financial crime - is ever increasing in complexity. What banks face now are new threats which they may not have answers to just yet. And, being the fiduciary agents in their capacity as banks, they realise their obligations also leave them open to potential lawsuits.

Banks and financial technology firms have a delicate balance to maintain. They have been increasing their investments in safer and more predictive technology systems to detect cases of fraud and money laundering. As financial controls tighten globally, money launderers have become even more sophisticated in their business.

The three main steps in money laundering (placement, layering and integration) already have several sub-steps within them, but money mules and asset purchases are giving way to more convoluted methods which seek to bypass detection.

Along with a steadfast use of KYC and regulations, financial institutions are increasingly turning to risk and compliance data and associated robotics process automation (RPA) and artificial intelligence (AI) to gain an advantage over potential financial criminals.

Data, automation and AI

In a recent Accenture report ("Banking Pulse Survey: Two Ways To Win"), 18 per cent of respondents said the main priority for the bank is to build security into the payments structure.

Meanwhile, 22 per cent cited AI, robotics, machine learning and innovative payments as the key platform technology capabilities required to scale up their core systems.

The monetary and physical strain that continuous compliance places on banks is enormous, which is why self-updating databases that promise to make the KYC processes more manageable are so attractive. Many banks have a variety of databases and watch lists to scan through when corroborating the identity and sources of funding and wealth of a potential client. These sources would include the FBI, Interpol and the UN, in conjunction with domestic sources of information. Given how quickly information is altered (by design or otherwise), these sources need to be automatically updated to maintain their authenticity and accuracy. Automating these processes with simple accelerator tools could go a long way in reducing processing time and improving productivity.

A typical anti money-laundering (AML) process is complex, intensive and time-consuming. It involves the monitoring of a customer's types and amount of transactions and the checking of historical alerts by accessing relevant data from multiple systems. There is also the review of the client's underlying transaction and KYC details and their transactional counter parties. In addition, public domain searches for negative information related to these customers and their counter-parties will also need to be performed.

A data-driven AML programme that leverages automation technologies like RPA (robotic process automation) creates a foundation for a more thorough risk-based approach towards determining AML risk that satisfies regulatory compliance and internal audit concerns as well in fraud detection.

Regulation and compliance in tandem

Before the 90s, financial institutions relied on a simple rules-based system to defend themselves against fraud. Rules-based solutions cannot keep pace with the highly dynamic nature of financial crime today. Nor can they deliver the immediate insight and predictive intelligence that can enable firms to actually stay one step ahead of the criminals instead of several paces behind.

With more innovative products and data sources than ever, the ability to continually discover emerging risks and new criminal patterns, coupled with the capacity to rapidly operationalise newly developed models into production, is a necessary requirement for modern financial crime platforms. In this environment, firms look to embrace graph analytics and machine learning to drive a smarter, risked-based approach to financial crime management.

An estimated US$800 billion to US$3 trillion is laundered globally each year. And it is said that a new banking regulation is created every 12 minutes across the globe. This begs the need for more sophisticated and agile forms of detection and enforcement in terms of AML and regulatory risks, as the scale and complexity of criminal activity grow.

As "false positive reduction" continues to be the priority for financial institutions, a judicious combination of advanced techniques, such as financial networks visualisation, transaction flow analytics and machine learning must be at the disposal of financial crimes data scientists. Further, financial crime and compliance management business and operational teams - from investigators to scenario testers - need tools to help them quickly understand, digest and act upon the findings produced by the data scientists.

Data analytics and machine learning tools are now increasingly being leveraged for the detection and reporting of such criminal activity. Banks' AML and anti-fraud compliance systems now look for deviations in transactions and analyse numerous levels of syntax to shed light on questionable activity.

The use of graph analytics is an emerging form of data analysis - the premise being that storing and managing data in the form of graphs adds to the rapid access to such data. More data can be added on quickly (without the need for additional modelling) and comes in particularly useful in detecting anomalies. These methods save resources, time and costs for banks and ensure a far deeper level of monitoring and speed than were previously available.

Many have also advocated the use of AI for scanning of multitudes of transactions and offering alternative criminal traits which may have eluded the first few monitoring passes. This is analogous to the current use of AI in retail banking where customers are offered suggestions on similar products or services based on buying or trading patterns. However, for these new frontiers to gain a measurable size of traction, a high quality and volume of available data would be required.

Cross-channel analytics and anomaly detection being fed into a machine learning matrix makes it seem like something out of a Terminator movie. But this future is only in its nascent stage - as those alarmed by this seemingly dystopian development heave a collective sigh of relief.

The writer is group vice-president for sales in JAPAC & the Middle East at Oracle Financial Services