Risk publications

AsiaRisk 25

AsiaRisk Awards 2020

Risk.net October 2020

Fraud detection and prevention product of the year

IBM®

Fraud detection and prevention product of the year

IBM

Banks typically rely on past patterns of behaviour to make predictions and detect fraud. But, as new patterns emerge, it is becoming a more complicated process. Adding to that is increasing online transaction volumes due to varying Covid-19 social distancing and lockdown measures worldwide.

Steven Scheurmann, regtech solutions leader for Asia-Pacific at IBM, says as fraud patterns are continuously getting more complex, thorough behavioural profiling and pattern recognition that can adapt quickly to new patterns is essential.

As new immediate payment schemes come to market, they create increasingly smaller time windows to determine if payments are fraudulent. "New payment schemes are competing for users with ease of use and therefore cannot afford high false-positive incidents that cause friction with users' experience," he says. Therefore, it is increasingly crucial for fraud analysts to assess the impact of payment model changes or new fraud countermeasures for millions of transactions, or more, within a few seconds.

IBM Safer Payments, a real-time payment fraud monitoring platform, helps financial institutions improve fraud detection and reduce false positives. It can accurately profile and monitor thousands of payments per second. It is equipped with various statistical and modelling tools that allow firms to build models that rapidly recognise and stop new or episodic payment fraud attacks. Safer Payments does this across diverse channel segments such as credit issuing and acquiring, immediate and alternative payments, and processors; and use cases such as card, non-card, cross-channel, online and more. It also protects multiple payment channels from sharing data between them.

The platform supports the import and export of fraud model components, which allow fraud analysts and data scientists to scale data science assets and build models. It also understands what the models are detecting and can explain why. The solution applies machine learning not only to train models but also to discover new rules that fraud analysts can test and integrate into the fraud detection engine.

Fraud professionals can build, test, validate and deploy machine learning models in a matter of days. The platform allows them to simulate and deploy new rules and models without interrupting monitoring. IBM Safer Payments leverages existing proprietary intellectual property with an open platform to allow external model and code ingestion. It is configurable through a web interface and is driven by the fraud professional, limiting vendor reliance or costly implementations.

Scoring models that are trained externally can be transferred to IBM Safer Payments as predictive model markup language (PMML) files. PMML is an open industry standard to exchange-scoring models. The scoring models are then computed in Safer Payments, and firms can run them with other model components using the virtual simulation "sandboxes".

An important distinction from other vendors is that IBM Safer Payments does not "rip and replace". It can integrate with and augment existing fraud detection solutions without impacting operational efficiency. Safer Payments is integrated with IBM Watson Studio to support rapid artificial intelligence (AI) model development. Watson Studio democratises machine learning and deep learning to accelerate AI implementations and provides a suite of tools and a collaborative environment for data scientists, developers and domain experts.

The solution, which has a microservice architecture, can either be deployed on site or on private or public clouds. IBM Safer Payments can run containerised workloads on multiple clouds using IBM's hybrid multi-cloud platform. It currently services more than 400 million customer accounts, more than five million merchants and half-a-million ATMs worldwide.

One of its recent clients is Volt Bank, an Australian digital bank, which integrated Safer Payments into its online banking platform in July this year. The solution is hosted on ISW's platform-as-a-service and provides Volt with safety and security features to give its clients a more seamless and secure banking experience. Bank of New Zealand (BNZ) also uses IBM Safer Payments to deliver cross-channel fraud protection to its customers and address the rising threat of crime and fraud. Fis announced at the end of 2019 that it is using IBM Safer Payments to protect its customers' peer-to-peer transactions. Four months after deployment, Fis recorded a 72% drop in fraud losses and a 90% drop in false positives.

IBM Safer Payments uses financial and non-financial data together with a customer's transaction history and performs authentication and profiling on each transaction. When it identifies potential fraudulent transactions, the transaction will be put on hold pending further validation.

Looking ahead, IBM will continue to add feature discovery capabilities to enhance the platform's model techniques further. As part of IBM Safer Payments' strategy to address firms incorporating enterprise-wide data for more accurate detection, IBM has native connectivity to open-source stream processing layers, data lakes and real-time data stores.

Scheurmann says IBM Safer Payments is leveraging IBM's investments in data and AI technologies to create a complete machine learning, financial crime management platform with explainable, actionable, advanced analytics. "IBM will continue providing banks, processors, card issuers and card acquirers of all sizes, around the world, with fraud prevention and anti-money laundering capabilities to manage risk, while improving customer experience in the most cost-effective manner," he says. ■