PLENUM
TECHNOLOGIES

Top Trends Shaping Fraud Management In Asia Pacific

TREND REPORT

March 17, 2022

Summary

A fragmented regulatory environment and the rapid transition to digital commerce have spurred several enterprise fraud management (EFM) trends in Asia Pacific (APAC). This report highlights key trends and changes in the EFM market in terms of changes in fraud patterns, customer preferences, and technology adoption. It provides actionable guidance to help security and risk (S&R) professionals in APAC respond to these trends.

Digital Transformations Have Caused An Explosion Of New Fraud Types

In Asia Pacific, the rapid transition to digital commerce and digital finance is a double-edged sword. While it has significantly improved customers' digital experiences and boosted the region's digital economy, it has left many systems and channels vulnerable to fraud. Rapid digital adoption also means that few merchants and financial institutions are prepared for a variety of novel and sophisticated fraud patterns such as promotion fraud, scams, group fraud, and the increasing convergence of fraud and money laundering. It can be seen that:

- **Digital commerce drives promotion fraud.** Flourishing digital commerce significantly changes consumer behavior, and companies are focusing their marketing spending on online campaigns and promotions. Fraudsters are increasingly taking advantage of these promotions, and the number of coupon hunters and fake accounts in APAC is growing significantly. Promotion and coupon fraud not only causes issues for brands and retailers but is also a headache for banks and other financial services firms. One large Asian bank said that about 15% of its fraud cases are promotion fraud.

- **Pandemic disruption engenders more group fraud.** A large Asian payment service provider told us that the pandemic has significantly disrupted the cash flow of some small- and medium-size merchants. As a result, many legitimate merchants have become fraudulent merchants — partnering with other fraudsters to initiate group fraud. Group fraud involves multiple types of financial crimes, like buyer and seller collusion fraud, merchant fraud, and money laundering.

- **Social engineering scams are growing fast.** Fraudsters increasingly use social engineering to conduct phone and online scams in APAC. Because transactions resulting from these scams are usually initiated by the social engineering victims (customers) themselves, it's difficult to prevent them with strong customer authentication alone. One Asian card network has seen a significant increase in such scams in recent years; as a result, it realized how important it is to efficiently share blacklist data such as phone numbers, IP addresses, and suspicious accounts across different organizations.

- **FRAML is gaining ground.** The increasing convergence fraud and money laundering that we see globally is also happening in APAC. A large Asian bank told us that it used to have separate fraud management and AML teams but recently began to consolidate some functions into a single team. This is because the increase in money laundering associated with fraudulent transactions requires fraud and AML teams to share information and collaborate more closely. Financial institutions in APAC are increasingly looking to converge EFM and AML into a single discipline: FRaud + AML = FRAML.

New Vendors, Third-Party Data Insights, And SaaS Are On Customers' Radar

The trends outlined above are causing companies in Asia Pacific to take the following actions:

- **Tech giants and payment firms are increasingly entering the EFM market.** In recent years, homegrown tech giants and digital platforms like Alibaba, Grab, and Tencent have announced new EFM offerings. Local payment companies such as 2C2P and Till Payments are increasingly adding EFM capabilities like tokenization and 3DS 2.0 authentication to their offerings. While these new players have some key advantages over traditional EFM vendors — including a deep understanding of business scenarios and massive volumes of consumer data and insights — competitive conflicts and concerns about sharing data with the services still exist. For instance, some e-commerce companies and retailers would have concerns using Alibaba's software as a service (SaaS)-based EFM solutions because of competitive conflicts. This applies to Grab and Tencent if they want to sell their solutions to competing platforms like Gojek and ByteDance.

- **Enterprises are demanding more third-party data and insights.** To lower customer friction and false positives, companies increasingly rely on third-party and consortium data such as IP address geolocation and reputation, blacklisted devices, and compromised passwords. EFM vendors that own a lot of consumer data — card networks like China UnionPay and digital platforms like Alibaba and Tencent — export risk scores based on fraud management insights from their own databases. Vendors that do not own and generate data themselves will collect (on a voluntary and client-by-client basis) tokenized/masked attributes such as name, phone number, address, and date of birth from known fraudulent transactions. These data sets help firms calculate a more reliable, context-aware fraud detection score.

- **Firms must decide between SaaS and on-premises.** Whether an APAC company prefers to adopt a SaaS or on-premises solution will vary by geography and industry. Firms in countries with stringent data residency and data security requirements, such as China and Indonesia, have less need for SaaS-based EFM solutions. Similarly, firms in highly regulated industries like financial services have a lower appetite for SaaS solutions than in industries such as retail and digital commerce. But as it becomes more necessary to use third-party data sources for EFM, we expect that the relevance of SaaS solutions will increase across APAC.

Keep An Eye On AI, Privacy-Preserving Tech, And Model-Building Platforms

The prevalence of sophisticated new patterns of fraud coupled with unique data residency and privacy requirements mean that firms in APAC need a more sophisticated set of EFM technologies and tools. The most critical EFM technologies and tools to watch in APAC are:

- **Sophisticated AI/ML-based models to respond to new fraud patterns quickly**. Machine learning (ML)-based models employing a variety of algorithms can effectively identify new fraud patterns and prevent different types of fraud. Models based on knowledge graph reveal and visualize complex relationships to battle group fraud and cryptocurrency fraud; Singapore-based vendor Cylynx used graph to help a crypto exchange monitor crypto transactions on blockchain by visualizing all transactions and the relationships behind them. Deep learning-based models can reliably predict fraudulent activity; Tencent's deep learning models enabled a large Chinese bank to improve its fraud prediction capabilities to prevent payment and loan fraud.

- **AI/ML model-building platforms to scale EFM usage.** The low-code and no-code trends are increasing customers' expectations of vendors to provide easy-to-use visual model-building features. This allows citizen data scientists and business users to build, train, and manage out-of-the-box and custom-built models and model ensembles. Vendors should provide capabilities for end users to build models based on rules, AI, and ML in an integrated, unified platform to improve data scientists' efficiency and augment business and nontechnical users' capabilities.

- **PPTs to augment data insights to fight fraud and stay compliant.** The rapid growth of digital financial services and lifestyle offerings require financial institutions to manage risk in a variety of channels and business scenarios, making it very valuable to get data insights from a breadth of sources. But regulations in many APAC countries forbid such institutions from exchanging data with external entities, including vendors — making it difficult to leverage data insights, such as risk scores, from vendors in a SaaS deployment model. To tackle this challenge, innovative vendors are developing privacy-preserving technologies (PPTs) like homomorphic encryption and federated learning. They help financial institutions enable federated data analytics projects while supporting the operationalization of privacy protection. Richer data insights from multiple channels and scenarios help them identify fraudulent transactions more effectively.

Collaboration And A Steady Flow Of Information Are Vital For EFM

Putting effective processes and tools in place for your organization's enterprise fraud management program is a must for it to be able to stay ahead of fraudsters and emerging fraud trends and remain competitive against its peers. Research recommends that S&R pros:

- **Consolidate and colocate EFM and AML staff to boost collaboration.** EFM and AML programs still suffer from being siloed. Leading financial institutions increasingly realize that EFM and AML use similar online access and transaction data; require similar heuristics and AI/ML techniques and tools for risk scoring and pattern identification; and employ similar investigative techniques. As a result, colocating EFM and AML teams, pursuing joint data integration projects, unifying model governance, and streamlining and consolidating investigation processes and tools helps to reduce FRAML costs.

- **Equip your EFM staff with the most updated fraud trends and patterns.** Some new fraud patterns, such as promotion fraud and group fraud, are unique to APAC. Firms need to keep a closer eye on these and educate their staff in a timely manner. They can leverage external vendors, especially those with a strong local presence and expertise, to get more information and help with avoiding losses. They can also use built-in patterns and models in SaaS-delivered EFM tools to cut model development time and data scientist labor cost.

- **Get assurances from your data provider regarding data privacy and protection.** Given recent high-profile fiascos and sanctions of firms violating data privacy laws, it's imperative that your organization only use vendor-supplied, consortium, or crowdsourced data that complies with local data privacy and residency regulations. These regulations often question or prohibit the use of device fingerprint and behavioral biometrics data and lists containing personally identifiable information such as names and addresses in cleartext.