Financial Fraud Trends in Asia - Pacific

June, 2026

Financial fraud across Asia is undergoing a significant transformation. The region has developed into a significant hub for increasingly complex fraud activities, with a 47% increase in fraud-related Notices and Diffusions between 2024 and 2025, according to INTERPOL's Global Financial Fraud Threat Assessment 2026. Fraud is no longer just isolated frauds carried out by lone offenders. Rather, criminal organisations run highly coordinated ecosystems that combine global money mule networks, cryptocurrency laundering, scam centres, and AI-enabled deceit. Financial fraud offenders and criminal organisations are becoming highly organised, skilled, flexible, and poly-criminals.

Key Financial Fraud Types

Investment Fraud: Some of the most substantial financial losses for individual victims are caused by investment fraud. Fraudsters use online platforms, such as criminal-controlled investment or trading apps, to manipulate people into investing their money in fake or misleading ventures. Fraudsters deceive the victims with false promises of high returns, misrepresenting investments and creating a sense of urgency. The trends within this type of fraud involve counterfeit virtual assets (crypto-investment scams) or fictitious real estate. The defrauded funds are frequently laundered through cryptocurrencies across South and Southeast Asia, making the recovery process of funds complex. Once the victim increases their investment, believing the scheme to be legitimate, the fraudster accesses the funds.

Impersonation Fraud: Offenders pose as individuals or institutions to manipulate victims into believing they're being investigated or are facing legal penalties. Over the past two years, this type of fraud has risen with the use of innovative technology like AI-generated images and videos blackmailing the victims to demand ransoms.

Business Email Compromise (BEC): BEC is a prevalent form of impersonation fraud. Criminals utilise techniques such as phishing kits and email spoofing, alongside personalised messages created via AI, to pose as trusted associates or corporate executives. These manipulative tactics are frequently employed to deceive individuals and organisations into authorising illicit wire transfers.

Romance Baiting Scam: Fraudsters in this scam integrate elements of romance fraud with crypto-investment deception. They first establish trust by contacting potential victims through social media, direct messages, or dating platforms. After gaining the victim's confidence, the criminals encourage them to participate in fraudulent investment opportunities, luring them with the prospect of high returns.

Emerging Fraud Trends

Quishing: With the rise in the usage of quick payment options, quishing is one of the rapidly growing financial fraud threats. Via email, SMS, public posters, digital advertisements, and online marketplaces, fraudsters distribute tampered QR codes that pose as authentic payment or transfer links. These codes trick people into entering their personal information, downloading malware, or approving fraudulent transactions by rerouting them to phoney websites that imitate real interfaces.

Growing use of Artificial Intelligence (AI): Several applications like generative AI, through which one can clone voices and faces in mere seconds, and Agentic AI autonomously plan and execute entire fraud schemes through profiling and surveillance of victims. Criminal networks offer end-to-end infrastructure, including phishing tools, fake trading platforms, AI-powered chatbots for victim grooming and encrypted communication channels.

Expansion of Scam Centres: Scam centres across the Asia - Pacific region use romantic scams and telecom fraud to target people. Victims of these schemes lose up to USD 83,000 in romance baiting cases and an average of USD 25,000 per telecom fraud incident. While traditionally these scam centres remained as a local phenomenon, this trend has now developed into a worldwide phenomenon. Many individuals are trafficked and held in scam centres and are being forced to commit fraud. The trend indicates that scam centres continue to grow more dangerous, sophisticated and widespread.

Hybrid Fraud Models: Fraudsters have been combining two or more fraud schemes, such as investment-sextortion and romance - sextortion schemes, to lure potential victims.

Risk Mitigation Measures

Enhanced Due Diligence (EDD): Once a customer is identified as high risk, financial institutions can adopt EDD measures, such as obtaining additional information on the business relationship, on intended or performed transactions, on the Source of Funds (SOF) or Source of Wealth (SOW) of the customer.

Transaction Monitoring: Financial institutions can monitor customer transactions to detect unusual patterns, rapid movement of funds, transactions inconsistent with a customer's profile, or activity involving high-risk jurisdictions. By analysing transactional behaviour in real time, institutions can detect potential fraud risks early and take timely action to prevent financial losses.

Early Warning Signals (EWS) Framework: Financial institutions can strengthen their fraud prevention by implementing EWS frameworks to identify potential fraud risks at an early stage. EWS mechanisms help detect unusual activity, sudden changes in transaction patterns, and behavioural anomalies. By identifying these warning signs, financial institutions can conduct further investigations and take preventive actions to mitigate the potential fraud risks.

Adverse Media Screening and Ongoing Monitoring: Institutions can identify possible connections to fraud, financial crime, sanctions violations, or other illegal activity by examining reliable news sources, regulatory actions, and publicly accessible data. Ongoing monitoring also helps to ensure that customer activities remain consistent with their risk profile and allows institutions to identify significant changes in behaviour, business activities, ownership structures, or risk exposure that may warrant further investigation.

Financial fraud in the Asia-Pacific region continues to grow in scale and sophistication, driven by evolving technologies, organised criminal networks, and increasingly complex fraud schemes. As fraudsters adopt new tactics such as AI-enabled deception and hybrid scams, financial institutions must strengthen their fraud prevention frameworks through effective due diligence, transaction monitoring, and ongoing screening to identify and mitigate emerging risks.

Quantum Data Engines™

Quantum Data Engines is a reg-tech company that helps financial institutions detect, manage, and report financial crime more effectively and efficiently.