# Responding to advancing financial fraud

Financial crime is on the rise, with cross-border money laundering and growth of fraud enabled by the accelerated adoption of digitalization and the ever-increasing sophistication of fraudsters blurring the line between cyber and financial crime.

The scale of the increase is demonstrated through global fraud detection and prevention market which is projected to grow from US$30.65 billion in 2022 to US$129.17 billion in 2029 (CAGR of 22.8 percent).[15]

Governments and regulatory entities around the world are responding, by enforcing robust regulation and shortening implementation timeframes. Saudi Arabia is keeping pace. In October 2022, SAMA issued its Counter-Fraud Framework to combat financial fraud in banks operating in the Kingdom.[16] This follows the issuance of instructions to all banks in April 2022 to implement several measures against financial frauds and to protect banking consumers.[17]

The framework has been developed to help banks to set up, implement, maintain, monitor, and improve effective counter-fraud controls with minimum standards for procedures and policies to prevent and detect fraud. General guidance themes include:

- Embedding fraud risk management into the bank's principal operation in the form of written policies, defined responsibilities, and on-going procedures that implement an effective program of fraud vigilance, detection, and prevention.
- Periodic assessment of the likelihood and impact of potential fraud schemes and the use of documented results to inform the design of the bank's fraud risk management program.
- Adoption of a comprehensive risk management system and system of internal controls, designed to prevent and detect fraud.
- Monitoring and reporting fraud incidents and trends, taking corrective actions as needed.

> SAMA's Counter-Fraud Framework is a welcome initiative to tackle bank-related fraud and will help the banking industry respond to the global trend of rising financial fraud.

### Technology is key to reducing financial crime

Effective utilization of technology is essential in the fight against fraud in the banking industry. The integration of fraud detection and protection (FDP) systems that use analytics, AI and machine learning are a critical weapon in the banking industry's armory against financial crime. According to a report by Juniper Research on online payment fraud, merchants and financial services organizations spent over US$9 billion on FDP solutions in 2022 (excluding identity theft, account takeover, or internal fraud) and the global FDP market size was estimated at US$25.66 billion in 2021.[18]

These systems use sophisticated technologies to detect and prevent fraud. AI and machine learning algorithms are trained to analyze transaction data and build profiles to identify patterns of fraudulent activity and flag suspicious transactions. Data and network analytics tools can automate and digitize data collection and analysis, combining information from multiple sources to improve the detection of anomalies or deviations in real-time and develop risk-based predictive models which can enrich and inform more accurate decision making. Predictive analytics can also be used to identify potential risks before fraud has even occurred with automated analytics utilized to detect anomalies across data entries and audit functions, providing an extra layer of detection in addition to traditional, manual selective checking techniques.

### ERP systems as the cornerstone of fraud mitigation

Another technology that is assisting banks with fraud are solutions based on Enterprise Resource Planning (ERP). These solutions not only help banks to increase their efficiency, agility, and profitability, they can play a major role in tackling financial crime through:

- Providing easy access to financial data across all departments and branches.
- Extending communication and collaboration between different units and locations.
- Enabling controls and monitoring of banking processes, risks, and compliance.
- Enforcing segregation of duties with strict authorization mechanisms throughout workflows.
- Automating repetitive tasks that assist in fraud detection and prevention.
- Analyzing data for improved detection.

### The human remains the weakest link

Despite all the efforts of regulators and the banking industry to shore up vulnerabilities with robust regulation, rigorous strategies, management systems and policies, and the adoption of FDP solutions, the customer remains a significant vulnerability. Fraudsters are using increasingly sophisticated psychological manipulation and techniques such as phishing, vishing, spear phishing, whaling, and business email compromise or interception. A recent addition is the growth of Authorized Push Payment (APP) fraud where the fraudster tricks the victim into willingly making an authorized transfer or payment rendering authentication ineffective. Authorized Push Payment (APP) fraud losses are on the rise and expected to climb to US$5.25 billion by 2026 (CAGR of 21 percent).[19]

Banks can partially tackle these types of fraud through monitoring transactions and behaviors for anomalies, implementing strong authentication and verification methods, and using advanced fraud detection and prevention solutions. However, novel threats remain an issue and education and awareness among customers is a necessity for the industry.

Banks should explore segmentation analysis that leverages fraud typology, victim demographics and geographic bias to assess specific vulnerabilities being exploited and target communications to customers accordingly. Targeted and tailored communication campaigns, aligned to current and emerging fraud threats, can deliver effective counter-fraud education and messaging to customers.

**Muhammad Talha**
Forensic Advisory
**E:** muhammadtalha@kpmg.com