Is artificial intelligence the new benchmark for financial crime risk management?

The Middle Eastern financial services industry (FSI) has experienced rapid growth in the post-pandemic era.[1] The initial lockdowns compelled financial institutions (FIs) to enable digital accessibility of their offerings to existing and prospective customers. This digital transformation, enacted in a short duration, led to the creation of risk that financial criminals have exploited.[2]

In response, FSI regulators in the Gulf Cooperation Council (GCC) have increased their efforts to combat rising financial crime risks. Recently, they have been encouraging market participants to integrate technologies into their respective financial crime control frameworks, issuing regulations and guidance to support FIs to effectively combat financial crime. Such directives include:

- The Central Bank of the United Arab Emirates (CBUAE) issued a guidance note encouraging FIs to use 'Digital ID' systems (referring to technology that uses electronic means to assert and prove a person's identity online and/or in in-person environments) to perform customer due diligence.[3]
- The Saudi Central Bank (SAMA) issued their 'Counter-Fraud Framework,' where it mandates FIs to define, approve, and implement a strategy for the sourcing/development and implementation of counter-fraud systems and technology to manage their fraud risks.[4]
- In its 'Anti-Money Laundering and Combating Terrorism Financing Instructions,' the Qatar Central Bank (QCB) mandates FIs to maintain sufficient resources, including technology, to effectively mitigate its respective financial crime risk.[5]

This article examines how FIs can integrate suitable anti-financial crime technologies in two key processes: identity verification and transaction monitoring.

Identity verification

The primary financial crime risk that FIs face when onboarding a new customer via their digital channels is impersonation fraud (i.e., an individual who poses as another to open an account; such accounts can then be used to facilitate criminal activity). FIs currently use controls such as multi-factor authentication (e.g., one-time-passwords, authentications apps) to mitigate the risk. However, financial criminals have found methods to defeat such controls.[6]

Advancements in technology, in the form of artificial intelligence (AI), now provide FIs with more sophisticated solutions that can be adopted to either complement or replace their existing controls that verify the identities of prospective and existing customers. Two such solutions include:

- **Identification document verification solutions:** FIs can integrate a solution that scans the prospective customer's live identification documents when uploaded onto the FI's digital channel via the prospective customer's mobile phone or computer to determine their validity and authenticity. This verification is performed through a variety of checks, such as hologram analysis, security patterns analysis, color analysis, and light and blur detection.
- **Biometric validation solutions:** FIs can integrate an advanced biometric validation solution, which verifies the identity of the prospective customer through numerous checks (e.g., facial recognition, liveness detection, age detection, gender detection, blinking analysis, mood analysis, behaviour analysis). Such tools can be customized in terms of the number of checks based on each FI's level of risk. Additionally, this technology can be leveraged to validate the identity of existing customers as well. For example, when a customer initiates a high-value transaction through a digital channel (i.e., mobile banking, online banking), an advanced biometric validation can be performed as confirmation the actual customer has actioned this.

Through such AI-driven solutions, FIs can significantly mitigate the risk of manipulation in their digital account opening and other identity verification processes. This technology can be leveraged to optimize financial crime compliance resources (e.g., replacement of one-time password OTP systems, re-purposing of manual reviewers) and provide cost benefits as well.

FSI regulators in the Gulf Cooperation Council (GCC) have increased their efforts to combat rising financial crime risks. Recently, they have been encouraging market participants to integrate technologies into their respective financial crime control frameworks, issuing regulations and guidance to support FIs to effectively combat financial crime.

Transaction Monitoring (TM)
As digital payment volumes surge in the region,[7] FIs are looking at ways to optimize their TM frameworks. Regulators such as the CBUAE have enabled FIs to explore dynamic intelligence-led TM models, which can enable FIs to identify wider networks in which customers operate instead of only individual transactions.[8] The current rules-based TM models to TM solutions adopted by FIs are only as effective as the quality of data feeding them.[9] The following are two AI-driven solutions that can augment the FIs' incumbent TM frameworks and support them in their TM optimization journeys:

- **Transaction analysis solutions:** FIs can integrate transaction analysis solutions, which can assess multiple data points linked to a transaction (e.g., transaction value, channel used, geographies involved, parties involved) to uncover highly complex and unusual patterns that may be linked to previously unknown financial crime schemes. This analysis can, subsequently, drive the TM system fine-tuning process in the form of updated scenarios, rules, and thresholds, and result in fewer false positives.

- **Specialized trade-based TM solutions:** FIs with higher volumes of trade-based business activity can integrate a specialized solution to detect trade-based money laundering. Such solutions can support the FI by automating large parts of the due diligence process (e.g., document extraction, verification, screening alerts, document image processing, document categorization, compliance checks, red flags, consistency check and text reconciliation) and providing additional protection against one of the most common methods of money laundering.

The inclusion of AI in the TM process can be a game-changer. Through proper implementation, manual tasks such as TM alert investigations (e.g., customer profile analysis, narrative development) can be automated, providing FIs time and cost efficiencies without any compromise on financial crime risk management. The adoption of such technologies will require a hybrid approach in initial phases, where technology performs labor-intensive tasks and humans provide oversight (including final decision-making), until intelligence-led TM models can prove to be more effective.

The use cases for AI-driven solutions are numerous, and their benefits are apparent (i.e., cost efficiencies, comprehensive reviews, time efficiencies, reduced errors, data-backed insights). In line with regulatory strategy across the Middle East, FIs should review their financial crime risk management strategies and consider making technology a focal component in order to realize the true benefits that AI can deliver for business and compliance. ●

By **Khushnood Khan**, Director, Financial Crime & Data Analytics and **Humaid Hussain**, Assistant Manager, Financial Crime & Data Analytics, Deloitte Middle East

In line with regulatory strategy across the Middle East, FIs should review their financial crime risk management strategies and consider making technology a focal component in order to realize the true benefits that AI can deliver for business and compliance

Endnotes

1. 'Middle East Banks Witnessing Digital Revolution,' Evalueserve, undated.
2. 'Financial crime risk rises in the Middle East and North Africa,' Refinitiv, 30 June 2021.
3. 'Guidance for Licensed Financial Institutions on Digital Identification for Customer Due Diligence,' CBUAE, 31 October 2022.
4. 'Counter-Fraud Framework,' SAMA, October 2022.
5. 'Anti-Money Laundering and Combating Terrorism Financing Instructions,' QCB, May 2020.
6. 'Scammers Are Cracking Today's More Secure Passwords — Here's What You Can Do,' Forbes, 25 July 2022.
7. 'Rise of Digital Payments in MENA Region: 2023 Digital Payment Trends,' Fintech News, 8 February 2023.
8. 'Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting,' CBUAE, 7 June 2021.
9. 'Transaction Monitoring Optimisation: Using an intelligence lead approach to Transaction Monitoring,' Deloitte, 2022.