Annex

What are the benefits of artificial intelligence in monitoring suspicious activities?

In recent years there has been an increasing trend towards adoption of artificial intelligence to help prevent and detect financial crime. Machine learning is one of the most common forms of artificial intelligence which some Authorized Institutions (AIs), taking into account the size and complexity of their businesses, have used to optimise the effectiveness and efficiency of anti-money laundering (AML) systems. These AIs have found that effective transaction monitoring requires finding the right balance between technology and human expertise to optimise processes. This note illustrates some of the benefits AIs can expect to see from using artificial intelligence, and should be read together with other guidance provided by the HKMA[1], which details how some of the challenges inherent to implementing artificial intelligence for AML can be overcome.

1. Wider data coverage (Effectiveness)

- In rules-based transaction monitoring (TM) systems, alert generation is mainly based on customers' existing transaction activities within certain prescribed periods (e.g. daily/ weekly/ monthly) *without* taking into account historical transaction activities outside these periods or other related contextual data from the subject customer.
- In contrast, the higher computing capabilities/ processing power in artificial intelligence-empowered monitoring systems enables the collation and analysis of vast amounts of data from various sources, which can greatly enhance AIs' detection capabilities for suspicious activity.
- Artificial intelligence has the capability to generate a much larger network of interrelated rules for different segments of an AI's customer portfolio. This can facilitate deeper insight, a more comprehensive and accurate assessment of a customer's ML/TF risk profile, and hence achieve a more effective outcome, providing the ability to identify suspicious patterns that may be difficult to spot in high volumes of data.
- Sources of data covered by artificial intelligence-empowered monitoring systems usually include:
    - AI's own data - data regarding the customer profile (e.g. obtained at on-boarding), transactions, previous alerts and results of any review or analysis, and where suspicious transaction reports (STRs) have been made within the AI's own system.

[1] HKMA Circulars "Report on AML/CFT Regtech: Case Studies and Insights Volume 1" issued on 21 January 2021, "Report on AML/CFT Regtech: Case Studies and Insights Volume 2" issued on 25 September 2023, and "Thematic Review of Transaction Monitoring Systems and Use of Artificial Intelligence" issued on 17 April 2024.

.

- External data - intelligence from financial institutions within the same banking group, law enforcement agencies, information sharing platforms (e.g. the FMLIT or FINEST [2] platforms) or watchlist information.

2. Enhanced detection capability (Effectiveness)

- Artificial intelligence-empowered monitoring systems are able to identify new typologies and detect complex networks of suspicious customers and their activities more effectively.
- The system also generates less noise and enables AIs to target higher-risk cases for investigation, freeing up resources of the AML function to focus on genuine high-risk cases. AIs which have adopted artificial intelligence-empowered monitoring systems have been able to achieve a higher STR conversion rate without compromising system effectiveness.

3. More timely follow-up action (Efficiency)

- Many AIs which have deployed artificial intelligence have cited addressing the overwhelming volume of false positive alerts, a long-standing industry pain point, as the primary driver. These alerts are not truly suspicious but must be cleared out of the queue, wasting valuable time and effort.
- The preliminary assessment results generated from an artificial intelligence-empowered monitoring system replace the different levels of initial assessment manually conducted by staff, thereby reducing overheads and, where implemented effectively with adequate testing and retraining of the model, significantly streamlining operations for alert handling and investigation.
- Artificial intelligence-empowered monitoring systems facilitate differentiation and prioritisation of cases of higher probability of financial crime for investigation and STR filing. Investigation of alerts generated from a purely rules-based TM system are consolidated into a holistic review on a customer-relationship basis, which can be conducted by a single investigator. This can shorten the overall time required for investigation, enabling the AI to mitigate the ML/TF risk sooner.

4. Improved sustainability (Effectiveness and Efficiency)

- Compared to rules-based TM systems which adopt static rules and parameters and require constant manual intervention for adjustment to cover the latest red

[2] FMLIT stands for Fraud and Money Laundering Intelligence Taskforce and FINEST stands for Financial Intelligence Evaluation Sharing Tool.

flags and typologies, an artificial intelligence-empowered monitoring system has embedded machine learning capabilities and can be trained on comprehensive data, customers' transaction activities and other parameters to detect more complex typologies and emerging risks.

- Manual rule-tuning to capture these emerging risks can be challenging, because codifying the new typology into quantifiable behaviours and then setting appropriate thresholds and segments takes time. Retraining an artificial intelligence empowered model can be much faster as there is no requirement to go through the whole cycle manually.

- New typologies and hidden patterns can then be identified through the AI's assessment of a customer's transactional activities. These new typologies, together with those shared by law enforcement agencies and through public private partnerships and intelligence from previous STRs, are fed into the model with a view to identifying similar patterns in the future, thereby enhancing detection capabilities in a more sustainable way.