HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B10/1C
             B1/15C

12 October 2023

The Chief Executive
28 Retail Banks

Dear Sir/Madam,

Enhanced approaches to combat digital fraud

I am writing to provide Authorized Institutions (AIs) with an update on enhancements being made to combat digital fraud and to communicate the expectation that these efforts should be adequately resourced and coordinated to ensure effective and efficient implementation and deliver stronger protection for customers.

The Hong Kong Monetary Authority (HKMA) continues to closely monitor the level of digital fraud and has prioritised work to help strengthen the banking sector's response. In the first nine months of 2023, the HKMA received 954 fraud-related banking complaints, exceeding the total of 555 cases for the whole of 2022, which is similar to the trend reported by the Hong Kong Police Force (HKPF)[1].

In light of these developments, the HKMA has worked with the industry to provide regulatory support, improve collaboration and promote innovation. These measures, including the five initiatives[2] announced by the HKMA with the HKPF and 28 retail banks in April 2023[3], will enhance anti-fraud efforts in the areas of information sharing, transaction monitoring and customer alerts.

---

[1] According to HKPF figures, the reported case number increased by 65% in the first quarter of 2023 and by 42% in the second quarter over the same period a year ago.

[2] The five anti-deception initiatives include real-time fraud monitoring, bank-to-bank information sharing platform, suspicious proxy identifier (ID) alert model, enhancement of 24/7 stop payment mechanism and assistance to investigation work of the HKPF.
(https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/04/20230421-7/)

[3] To support implementation by banks, "Guidance Notes on the Implementation of Anti-Deception Initiatives (Guidance Notes)" was issued in May 2023.

A.   Information Sharing

Fraud and Money Laundering Intelligence Taskforce (FMLIT)

FMLIT has been delivering significant results since inception in 2017, by sharing information between the public and private sectors. To build on this success and widen the scope of FMLIT, participation has been expanded to include 28 retail banks and six Stored Value Facility (SVF) Licensees will join later this year. The HKMA will continue to monitor how AIs use FMLIT data and apply analytics and other Regtech capabilities to contribute to FMLIT intelligence and analysis. AIs are expected to allocate adequate resources to support this effort.

Bank-to-bank information sharing platform

To increase the ability of banks to share timely financial crime risk information with other banks and take swift mitigating measures, the pilot phase of the Financial Intelligence Evaluation Sharing Tool (FINEST) was rolled out in June 2023, covering five domestic systemically important Authorized Institutions (D-SIBs) sharing information on corporates suspected to be involved in fraud-related money laundering activities. Based on the experience of the pilot phase and making reference to international experience, FINEST will be expanded to cover more banks and a wider scope of financial crimes and accounts. The HKMA will soon consult the industry and the public on legal provisions to facilitate personal account information sharing for preventing and detecting crime.

B.   Transaction Monitoring – Real-time Fraud Monitoring System

Given the increase in deception cases, often involving exploitation of new and emerging technology, it is imperative that AIs deploy innovative solutions to combat fraud. In line with the HKMA's requirements, 28 retail banks have all implemented real-time fraud monitoring and detection capabilities, including the ability to alert customers whenever a high-risk transaction is identified.

Examples of how AIs may strengthen efforts in real-time fraud monitoring by applying network analytics have been provided in Anti-Money Laundering (AML) Regtech Lab (AMLab) events[4] and in HKMA publications[5]. AIs should further explore the inclusion of more data and applying network analytics in real-time fraud monitoring systems to strengthen their ability to identify high-risk accounts and networks and alert customers of high-risk transactions.

---

[4] Two AMLabs covering the theme network analytics were held in November 2021 and November 2022 respectively. For details, please refer to the press releases:
https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/11/20211105-6/
https://www.hkma.gov.hk/eng/news-and-media/press-releases/2022/11/20221124-3/
[5] "AML Regtech: Network Analytics"
(https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/05/20230509-3/)
"AML/CFT Regtech: Case Studies and Insights Volume 2"
(https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/09/20230925-3/)

C.   Customer Alerts – Faster Payment System (FPS) Suspicious Proxy ID Alert Model

The anti-fraud search engine "Scameter" was launched in September 2022, enabling the public to check whether a transaction may be at higher risk for fraud. The HKMA is now working with AIs, SVF Licensees, the HKPF and Hong Kong Interbank Clearing Limited to introduce a pre-transaction alert mechanism for FPS transactions, based on Scameter information, which will alert customers where the FPS Proxy ID of the payee is listed as "High Risk" in the Scameter engine, giving them an opportunity to further verify, and where necessary stop, the payment. In order to effectively implement the Suspicious Proxy ID Alert Model across all FPS participating AIs and SVF Licensees in the coming two months, AIs are required to make appropriate system enhancements and communicate these changes to customers in good time, making reference to the relevant circulars and communication materials issued and/or updated by the HKMA from time to time.

AIs are expected to establish adequate systems and controls with senior management oversight to enable effective implementation of the measures and initiatives. The objectives and requirements should be clearly communicated to staff and key performance indicators should be developed to track performance. The HKMA will collect related data from AIs and review the effectiveness at implementation and as part of ongoing supervision.

The HKMA will continue to work closely with banks and all stakeholders to enhance the ecosystem response to the evolving threat from fraud and financial crime. Should you have any questions regarding this circular, please contact us at aml@hkma.iclnet.hk.

Yours faithfully,

Carmen Chu
Executive Director (Enforcement and AML)