



HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B10/1C
B1/15C

20 December 2024

The Chief Executive
All Retail Banks

Dear Sir/Madam,

Measures to protect bank customers from authorized payment scams

I am writing to provide Authorized Institutions (AIs) with guidance on the measures they should put in place to prevent, detect and disrupt authorized payment scams (APS)¹.

The Hong Kong Monetary Authority (HKMA) continues to closely monitor the levels of frauds and scams in Hong Kong. According to the statistics published by the Hong Kong Police Force (HKPF), the number of deception cases increased from around 8,000 in 2018 to nearly 40,000 in 2023 with total losses exceeding HK\$9 billion last year. In the first 10 months of 2024, around 36,000 deception cases were reported, representing an increase of 7% over the same period last year.

To strengthen the industry response, the HKMA has taken a number of initiatives, including comprehensive packages of e-banking and payment card security measures and five anti-deception initiatives rolled out jointly with the HKPF in 2023². Following the implementation of these measures, the total number of banking complaints dropped notably by 35% in the first 10 months of 2024. However, the number of banking complaints related to APS remains high, despite an overall decline of 18% during the same period.

The HKMA therefore considers that there is a need for AIs to ensure measures are both proactive and effective in protecting their customers from APS. The package of measures set out below are formulated after consultation with selected AIs and the HKPF as well as reference to overseas practices.

¹ APS refer to scams in which customers are deceived into authorising payments from bank accounts.

² Set out in the HKMA's circulars on "[Binding Payment Cards for Contactless Mobile Payments](#)" dated 25 April 2023; "[Major Enhancements on Protection of Payment Card Customers](#)" dated 20 June 2023; "[Enhanced approaches to combat digital fraud](#)" dated 12 October 2023 and "[Enhancement to security of electronic banking services](#)" dated 31 October 2023.

1. Comprehensive framework to tackle APS

AIs should establish an effective framework, including appropriate policies and procedures, to detect, deter and disrupt APS. The framework should be subject to adequate oversight by senior management, sufficiently resourced, including staff with relevant experience and training covering the latest scam trends and typologies published by the HKPF and the HKMA.

2. Dynamic APS monitoring system in response to evolving typologies and risk indicators

An AI's APS monitoring system (which can form part of an existing fraud and scam monitoring system or a separate system) should be capable of identifying high-risk situations or indicators of APS and, at a minimum, take into account customer risk profile, banking behaviour, transactional information, the latest scam trends and typologies as well as external intelligence on suspicious account information, including that received through information sharing platforms (e.g. the Fraud and Money Laundering Intelligence Taskforce or FMLIT).

3. Prompt handling of customer alerts

Where a high-risk situation is identified or an alert is generated by the APS monitoring system, AIs should promptly alert customers to the risks and confirm whether they wish to proceed with the transaction concerned. During the process, AIs should raise suitable questions with the customers to probe the purpose and nature of the transaction concerned (in particular the beneficiary and the customer's knowledge of and/or relationship with him/her) and assess whether the explanation provided is commensurate with the AIs' knowledge of the customer's profile, given the circumstances. The follow-up actions should adequately address the assessed level of risk.

4. Effective risk mitigating measures

Where customers decide to proceed with the transaction regardless of alerts from AIs or cannot be contacted, AIs should seek appropriate advice and assistance from the HKPF. In situations where AIs have reasons to believe that it is highly likely that a customer is falling prey to a scam, they should consider taking further mitigating measures such as holding the transaction temporarily while requesting the customer to contact them or assessing the need for HKPF involvement.

AIs should provide a convenient and easily accessible channel for customers to seek and obtain help with respect to potential APS.

5. Sharing of intelligence and use of technology

AIs should consider sharing suspicious account information and typologies with other AIs through established gateways such as FINEST³ and effectively utilize

³ FINEST stands for Financial Intelligence Evaluation Sharing Tool, a bank-to-bank information sharing platform launched in June 2023.

the shared intelligence received from other AIs or the HKPF. They are encouraged to proactively share strategic insights and exchange tactical intelligence as well as developing and exchanging the latest typologies and related mitigating measures through FMLIT.

AIs should give due consideration to adopting artificial intelligence and network analytics in their APS monitoring systems to enable more effective detection of complex networks of suspicious accounts and activities.

6. Proactive participation in anti-deception initiatives

The five joint anti-deception initiatives play an important role in combating APS and AIs should monitor their performance in these initiatives. For example, in order to swiftly identify and intercept crime proceeds and proactively alert potential scam victims, AIs should, on an ongoing basis, seek to enhance effectiveness and efficiency in handling requests from the “24/7 Stop Payment Mechanism” and the upstream scam intervention mechanism operated by the Anti-Deception Coordination Centre. The HKMA will collect and review performance-related data and provide feedback to individual AIs where appropriate.

7. Publicity and education

While the HKMA expects AIs to implement effective measures to prevent, detect and disrupt APS, customers have a fundamental responsibility for protecting themselves from falling prey to scams. To maximise publicity efforts, AIs are expected to work closely with the HKMA and the HKPF and deliver timely educational messages on the latest scam tactics to alert their customers.

AIs should review existing frameworks and implement the aforementioned measures as soon as practicable, and in any case no later than 30 June 2025. If AIs encounter practical difficulties or have any questions related to this circular, they may approach their usual supervisory contact at the HKMA’s AML and Financial Crime Risk Division.

Yours faithfully,

Raymond Chan
Executive Director (Enforcement and AML)