HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

31 October 2023

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Enhancement to security of electronic banking services

We are writing to require authorized institutions (AIs) to implement a package of new enhancement measures, formulated by the Hong Kong Monetary Authority (HKMA) in consultation with the Hong Kong Association of Banks (HKAB) and the Hong Kong Police Force, to further strengthen the security of electronic banking (e-banking) services.

As digitalisation and innovative banking services bring new levels of convenience to customers, they also create additional avenues for fraudsters to commit digital crimes. According to statistics compiled by the Police, the number of technology crime cases reported in the first half of 2023 reached 15,000, representing an increase of 47% over the same period last year. A similar increase is also observed in the numbers of fraudulent websites, phishing emails, and other scams reported by AIs to the HKMA.

Against this backdrop, the HKMA keeps its supervisory requirements on e-banking and other digital services under constant review. Earlier this year, the HKMA's conduct and prudential supervisory teams jointly developed a package of measures to strengthen the security of payment card services. These measures are contained in the circulars "Binding Payment Cards for Contactless Mobile Payments" and "Major Enhancements on Protection of Payment Card Customers", issued on 25 April 2023 and 20 June 2023 respectively.

In parallel with the above efforts, the HKMA has formulated a set of additional measures, in collaboration with HKAB and the Police, to strengthen the security of e-banking. These measures aim to increase the protection for bank customers

against fraudsters seeking to conduct unauthorised transactions through e-banking accounts. Details of these measures are set out below:

I. Enhanced monitoring for suspicious transactions and additional customer authentication to counter frauds

1. Dynamic fraud monitoring mechanism – In light of the growing sophistication of deception tactics, AIs should establish dynamic fraud monitoring rules incorporating the latest threat intelligence and customers' historical data and transaction patterns. These rules should encompass a broad spectrum of risk factors, including but not limited to, geographical locations of logins, the time between successive logins and the value of the requested transaction. To bolster fraud detection capabilities, scam intelligence sources (e.g. Scameter) and network analytics tools should be used to promptly identify suspicious transactions and accounts and generate timely alerts to customers.

2. Ambush authentication – If suspicious e-banking activities are detected (e.g. access from suspicious IP addresses or device IDs), AIs should deploy ambush authentication following a risk-based approach to verify the identity of the person operating the e-banking account. This measure, if properly designed, can make it substantially more difficult for fraudsters to conduct unauthorised transactions. AIs should take appropriate follow-up actions, such as account lock-out and sending notifications to customers, in cases of multiple authentication failures.

3. Additional confirmation for suspicious high-risk transactions – High-risk e-banking transactions are currently subject to two-factor authentication as stated in the Supervisory Policy Manual (SPM) module TM-E-1 on "Risk Management of E-banking". Where high-risk e-banking transactions are assessed to be suspicious by AIs (e.g. large-value fund transfer shortly after device binding), AIs should request the customer to provide an additional confirmation (e.g. in-App confirmation or callback) prior to executing the transaction.

4. Capability to implement multiple authentication methods – As stated in SPM module TM-E-1, AIs are required to adopt effective authentication methods to verify the identity of a customer. As fraudsters continually adapt their tactics, multiple authentication methods are essential for countering different modus operandi (e.g. use of facial recognition to reduce phishing risk and soft tokens to address the risk of SIM swapping). AIs should therefore maintain the capability to implement multiple authentication methods commensurate with the evolving risk landscape.

II. Empowering customers to safeguard bank accounts

5. Review of e-banking activities – To facilitate early detection of unauthorised e-banking activities, AIs should provide customers with tools that empower them to review and monitor account activities. These tools should make available detailed information such as the login date and time, geographical location and device information relating to a transaction, allowing customers to promptly identify suspicious access to their e-banking accounts. In addition, these tools should permit customers to perform searches for high-risk activities such as activation of device binding.

6. Notification of unusual e-banking activities – In addition to notifying customers of high-risk transactions, AIs should conduct risk assessments and broaden the scope of notifications to include unusual e-banking activities (e.g. changes in geographical locations, use of new devices and new login behaviour). Such notifications can help customers detect suspicious activities over their bank accounts early.

7. Lowering default cross-border funds transfer limits – As it is common for fraudsters to transfer a victim's money out of Hong Kong, AIs should permit customers to set a lower default cross-border transfer limit. Requests to increase the cross-border transfer limit should normally be regarded as high-risk transactions.

8. Restricting concurrent login sessions – To guard against unauthorised access, AIs should put in place session management controls that disallow concurrent logins to an e-banking account. Key data such as IP address, device type, and geographical location of the additional login attempts should be logged for auditing and threat analysis purposes.

III. Containing damage to customers in case of serious breaches

9. Suspension of bank accounts – However robust the defence of banks is, the possibility of a customer's e-banking account being compromised by fraudsters cannot be ruled out. To contain the damage to customers in such cases, AIs should provide a mechanism for customers to promptly suspend their e-banking accounts. The mechanism can be in the form of a dedicated hotline or an easily accessible function available on internet banking or mobile banking applications. Once a bank account is suspended, appropriately stringent customer authentication should be performed before the customer's e-banking account is reactivated.

10. Maintaining a 24/7 customer reporting channel – To facilitate customers to report suspicious banking activities or potential fraud, AIs should offer a convenient and accessible channel (e.g. through mobile banking applications or other effective means) for customers to seek and obtain help.

Apart from the above enhancement measures, the HKMA will continue its consumer education efforts to promote public awareness of e-banking frauds. AIs are expected to actively participate in and contribute to these efforts.

AIs should implement the aforementioned e-banking enhancements as soon as practicable, and in any case no later than 31 March 2024. Given that AIs are currently implementing other enhancement measures to counter digital fraud, including those relating to payment card protection, the HKMA is prepared to exercise flexibility where an AI has genuine practical difficulties in observing this implementation timeline.

The HKMA will revise SPM module TM-E-1 to incorporate the above new enhancement measures, as well as those relating to payment card security, into its e-banking guidelines. Industry consultation on the amendments will be undertaken in the next few months.

Should you have any questions about this circular, please feel free to contact Mr Tsz-Wai Chiu on 2878 1389 or Mr Kevin Yau on 2878 1044.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)