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

14 April 2025

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

New Anti-Digital Fraud Measures: "E-Banking Security ABC"

I am writing to set out the enhancements expected to be implemented by Authorized Institutions (AIs) to further strengthen the security of E-banking, for better protecting the public from evolving digital fraud trends. In tandem, the Hong Kong Monetary Authority (HKMA) will continue to work closely with the banking industry in raising public awareness of the latest modus operandi of frauds and scams, and empowering bank customers to embrace "E-Banking Security ABC", that is, "**A**uthenticate in-App, **B**ye to unused functions, **C**ancel suspicious payments".

The HKMA has been closely monitoring the digital fraud landscape and actively guiding AIs to implement effective measures to address emerging threats, as well as promoting customer awareness. For instance, noting a growing propensity for fraudsters to target online payment card transactions globally, the HKMA has required AIs since late 2024 to allow customers to authenticate these transactions via a bound device by default, rather than using SMS One-Time-Passwords (OTPs). Card-issuing banks in Hong Kong that implemented the measure saw a nearly 80% reduction in fraud rates since then. In addition, the HKMA, working with the banking industry and the Hong Kong Police Force (HKPF), expanded the Suspicious Account Alert mechanism[1] to cover the majority of the public's day-to-day payment transfers. In the second half of 2024, over 50,000 alerts were issued, providing a tangible basis for customers to think twice about high risk transactions.

/…Page 2

[1] For more details, please see the HKMA's press release "Expansion of Suspicious Account Alert for Automated Teller Machine transactions" of December 2024.

While these measures have remained largely relevant to-date, the HKMA notes that the modus operandi of fraudsters continue to evolve rapidly. In particular, there are early signs that some bad actors may have tried to leverage advanced technologies, including artificial intelligence and deepfake in particular, to enhance the sophistication of their deception techniques.

Adopting a forward-looking approach, the HKMA is introducing three enhancements to E-banking security measures, which are designed in consultation with the HKPF and the Hong Kong Association of Banks (HKAB) to address the evolving risks. In practical terms, AIs should provide convenient means for customers to:

- **"<u>A</u>uthenticate in-App"** – Facilitate customers to adopt bound devices by default, instead of SMS OTPs, for authenticating specified Internet banking activities, including logins to Internet banking and high risk transactions (e.g. fund transfers to unregistered third parties);

- **"<u>B</u>ye to unused functions"** – Empower customers to make own choice of deactivating higher risk functions in Internet banking, using a phased approach as appropriate, and starting with two functions, namely online increase of transfer limits and online registration of third-party payees; and

- **"<u>C</u>ancel suspicious payments"** – Further enhance the effectiveness of alerts displayed under the Suspicious Account Alert mechanism, including by adjusting their duration and content.

The HKMA's supervisory expectations for each of these enhancements, which are intended to be implemented by AIs for all retail bank customers[2], are set out in details in the **<u>Annex</u>**. AIs should endeavour to meet the implementation timelines, while we stand ready to discuss with individual AIs on alternative proposals and mitigation measures should any AI encounters genuine difficulties.

/…Page 3

[2] Although these measures target individual customers of retail banks, AIs are encouraged to consider extending them to other types of customers (e.g. business customers and private bank customers) as appropriate, especially where the nature of transactions conducted by these customers may bear similarities with retail banking.

In parallel, the HKMA will also continue to uplift AIs' ability to manage risks stemming from emerging technologies, including deepfakes. Building on the success of our earlier anti-digital fraud workshop[3], as well as insights drawn from our GenA.I. Sandbox, we will issue further guidance to elevate the ecosystem's readiness to combat deepfake-enabled modus operandi.

To ensure that customers are able to effectively leverage the new measures to defend against digital frauds and scams, AIs should clearly communicate the implementation specifics (e.g. the details of "cooling-off" periods or other enhanced risk management controls that may be applied) to customers in easy-to-understand language. In tandem, the HKMA will continue to strengthen consumer education around "E-Banking Security ABC" and will look to AIs to actively contribute to, and join hands with us to empower better customer protection.

Should you have any questions regarding this circular, please address them to ebanking@hkma.iclnet.hk.

Yours faithfully,

Carmen Chu
Executive Director (Banking Supervision)

[3] The HKMA jointly held with the HKPF, Digital Policy Office and HKAB an anti-digital fraud workshop on 13 November 2024 to raise industry awareness of fraudsters' use of deepfakes and to share good practices for managing the associated risks. More than 140 participants from 70 AIs joined the workshop.