HONG KONG MONETARY AUTHORITY
香港金融管理局

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

25 August 2025

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

<u>"E-Banking Security ABCD"</u>

I am writing to provide guidance on the enhancements to E-Banking security measures [1] to cover deepfake defence tactics, with immediate effect. It is accordingly rebranded as "E-Banking Security ABC**D**" – "**<u>A</u>**uthenticate In-App", "**<u>B</u>**ye to unused functions", "**<u>C</u>**ancel suspicious payments", "**<u>D</u>**eepfake detection".

The Hong Kong Monetary Authority (HKMA) has been closely monitoring the evolving fraud risks posed by deepfake technology. Progressive actions are being taken – including with the support of expert partners – to strengthen the Hong Kong banking sector's capability to combat deepfake-related modus operandi, especially those targeting the identity verification solutions deployed by banks.

As part of these efforts, we launched the Generative Artificial Intelligence (GenA.I.) Sandbox[2] in collaboration with the Hong Kong Cyberport Management Company Limited (Cyberport) in August 2024, hosted an Anti-Digital Fraud Workshop with the Hong Kong Police Force (HKPF), Digital Policy Office and Hong Kong Association of Banks in November 2024, and also unveiled a new GenA.I. Collaboratory series, under which a tailored cross-sectoral engagement session was held in July 2025 to bring together digital banks and technology firms to discuss the latest deepfake developments and effective prevention solutions.

/…Page 2

[1] Please refer to the HKMA's circular on "New Anti-Digital Fraud Measures: "E-Banking Security ABC"".
[2] Please refer to the HKMA's press release on "HKMA and Cyberport Launch GenA.I. Sandbox to Bolster A.I. Adoption in Financial Sector".

Authorized institutions (AIs) have participated actively in these initiatives and also taken onboard the insights and learnings shared. Notably, some AIs successfully tested different anti-deepfake solutions under the first cohort of the GenA.I. Sandbox, while others have followed the advice provided by the HKMA at the Anti-Digital Fraud Workshop to implement advanced deepfake detection solutions. Our regular engagement with AIs showed that those which adopted relevant solutions, and related good practices (as summarised in the **Annex**), improved their capability to detect sophisticated, real-time deepfake attacks by more than 95% in number. The benefits extended across the ecosystem, as the identified fraud and scam cases have been shared by AIs with the HKPF, and facilitated law enforcement investigations as well as the early identification of emerging deepfake-related tactics before further proliferation.

Noting the positive outcomes so far, and as the first initiative under Measure "D", the HKMA expects AIs to review the relevance of the good practices to their institution and take appropriate action(s) to step up their deepfake detection capabilities.

Going forward, the HKMA will continue to launch new initiatives under Measure "D". Besides keeping the good practices under regular review, the HKMA will provide practical utilities to enhance AIs' anti-deepfake capabilities. In particular, the second cohort of the GenA.I. Sandbox is currently open for applications with the theme of "A.I. versus A.I.", and will allow AIs to examine how to use A.I. technology to combat the risks and threats elevated by A.I. advancements, including the emergence of deepfakes. Applications are welcome until the deadline of 31 August 2025[3], and the resultant insights will also be shared in future GenA.I. Collaboratory sessions and/or in the form of further practical guidance, as appropriate.

Leveraging on the Memorandum of Understanding (MoU)[4] signed between the HKMA and the School of Business and Management of the Hong Kong University of Science and Technology in May 2025, efforts will also be made to deliver resources that support growth in the industry's anti-deepfake capabilities. More details will be announced in due course.

/…Page 3

[3] More details about the application process can be found in the HKMA's circular on "Generative Artificial Intelligence Sandbox: Second Cohort".
[4] For details, please refer to the HKMA's press release on "HKMA and HKUST sign MoU to advance cybersecurity innovation for Hong Kong's financial sector".

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

Yours faithfully,

Carmen Chu
Executive Director (Banking Supervision)