Our Ref.: B10/1C
B1/15C
B10/21C

3 September 2026

The Chief Executive
All Authorized Institutions and Stored Value Facility Licensees

Dear Sir/Madam,

Remote on-boarding of individual customers

I am writing to update the Hong Kong Monetary Authority's (HKMA) regulatory expectations regarding remote customer on-boarding, taking into account the widespread adoption of remote on-boarding solutions driven by rapid technological innovation in recent years. This circular supersedes the circulars on "Remote on-boarding of individual customers" issued on 1 February 2019 and "Remote on-boarding and iAM Smart" issued on 24 May 2021. The circulars on "Remote onboarding of corporate customers" dated 24 September 2020 and "Feedback from recent thematic reviews of Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) control measures for remote customer on-boarding initiatives" dated 3 June 2020 continue to be applicable and should be read in conjunction with this letter.

Remote on-boarding solutions have now become an integral part of the AML/CFT controls of Authorized Institutions (AIs) and Stored Value Facility (SVF) licensees. At the same time, advancements in technology have also driven changes in the money laundering and terrorist financing (ML/TF) risk landscape. In particular, artificial intelligence driven automation and sophisticated tactics, including the use of deepfake technology, have increased the potential for impersonation, online fraud and associated mule-account networks at much greater scale.

To address these threats effectively, the HKMA has been working closely with the industry and the Hong Kong Police Force to share the latest tactics and modus operandi with AIs and SVF licensees, which are expected to use that intelligence to ensure, on an ongoing basis, that their systems and processes can effectively mitigate both existing and evolving ML/TF risks. This applies particularly to remote on-boarding solutions, which should be subject to a continual program of updates and recalibration in order to remain effective and compliant with two core principles:

(i) identity authentication – where the individual customer's identity is obtained through electronic channels, AIs and SVF licensees should take appropriate measures to ensure reliability of the document, data or information obtained for the purpose of verifying the customer's identity. This includes utilising technology to ascertain the genuineness of the identity document; and

(ii) identity matching – AIs and SVF licensees should use appropriate technology to link the customer incontrovertibly to the identity provided in (i).

In addition to complying with these core principles, AIs and SVF licensees are expected to adopt a risk-based approach in the design of their products and services that should be proportionate to the customer's assessed ML/TF risk profile. For example, a tiered approach enables account features, functionality and transaction limits to be scaled dynamically and adjusted according to actual usage and ongoing customer behaviour. When combined with robust remote on-boarding solutions and active senior management oversight, such an approach can significantly strengthen AML/CFT controls.

AIs and SVF licensees should conduct a comprehensive review of their remote on-boarding solutions, and the systems and oversight to ensure their ongoing effectiveness, taking into account the latest intelligence about fraud and scam tactics shared by the HKMA and the Hong Kong Police Force.

If AIs and SVF licensees have any questions about this circular, they may approach their usual contact at the HKMA's AML and Financial Crime Risk Division.

Yours faithfully,

Raymond Chan
Executive Director (Enforcement and AML)