



HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B10/1C
B1/15C

24 May 2021

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Remote on-boarding and iAM Smart

Our letter of 1 February 2019¹ highlighted two key principles, i.e. identity authentication and identity matching, in the use of technology. I am writing to provide further elaboration to encourage the wider adoption of iAM Smart² in remote on-boarding arrangements to enhance effectiveness.

Consistent with the Financial Action Task Force (FATF) standards and the Guidance on Digital Identity published by the FATF in March 2020³, the identity verification requirements⁴ as set out in the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT Guideline) are sufficiently flexible to allow Authorized Institutions (AIs) to on-board customers remotely. As clarified in our 2019 letter, iAM Smart is an acceptable technology solution to meet these requirements and some AIs have already started testing remote on-boarding initiatives using iAM Smart, and others are considering similar initiatives.

¹ HKMA Circular “Remote on-boarding of individual customers” issued on 1 February 2019 (<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190201e1.pdf>)

² iAM Smart was launched in December 2020 by the Office of the Government Chief Information Officer as one of the key infrastructure projects for smart city development announced in the 2017 Policy Address. It provides all Hong Kong residents with a single digital identity and authentication to conduct government and commercial transactions online.

³ The paper can be found at: (<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf>)

⁴ To verify the customer’s identity by reference to documents, data or information provided by a reliable and independent source.

In light of these developments and based on feedback received in the HKMA Fintech Supervisory Sandbox (FSS) and Chatroom, the Hong Kong Association of Banks (HKAB), with input from the HKMA, has updated the Frequently Asked Questions (FAQs) in relation to AML/CFT to help AIs understand how iAM Smart can be used in complying with the relevant AML/CFT requirements. For example, the FAQs clarify that when iAM Smart is used for identity verification, record keeping requirements may be met by retaining the specific data or information obtained from iAM Smart through Application Programming Interface, showing the customer's iAM Smart authentication result and verified Hong Kong Identity Card data. AIs do not need to obtain additional identification documents solely for record keeping purposes. The updated set of FAQs is available on the websites of the HKAB and the HKMA.

AIs considering using iAM Smart to facilitate remote customer on-boarding or support ongoing due diligence may make reference to these FAQs, together with all relevant guidance including the AML/CFT Guideline. AIs are also reminded to apply a risk-based approach when conducting customer due diligence (CDD) and that the extent of CDD measures should be commensurate with the money laundering and terrorist financing risks associated with a business relationship.

The HKMA has been, and will continue to be, working closely with the industry to promote the greater use of technology, including remote on-boarding initiatives, to enhance the efficiency of AIs' CDD processes and improve customer experience. We also welcome AIs to discuss with us any remote on-boarding proposals, including those using iAM Smart, through the HKMA FSS and Chatroom.

Should you have any questions regarding this letter, please contact us at aml@hkma.iclnet.hk.

Yours faithfully,

Carmen Chu
Executive Director (Enforcement and AML)