HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B10/1C
B1/15C

24 September 2020

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Remote on-boarding of corporate customers

Further to our letter of 7 April 2020 which encourages, among others, measures that can provide greater convenience for account opening and continued access to banking services during COVID-19, I am writing to articulate key principles in relation to remote on-boarding of corporate customers based on use cases and proposals gathered through our ongoing engagement with the industry. This circular reflects the regulatory expectations set out in the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) and the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) (AML/CFT Guideline).

Unlike on-boarding of individual customers, a business relationship with a corporate is generally established through its representative(s) with appropriate authority to act on behalf of the corporate. Customer due diligence (CDD) is more extensive compared with individuals and typically involves a number of steps[1], including for example:

(i) verification of the corporate's identity;
(ii) verification of the identity of the corporate's representative(s) and related authority[2];
(iii) verification of beneficial owners' identities; and
(iv) understanding the ownership and control structure as well as the nature of business of the corporate etc.

[1] Reference can be made to the CDD requirements stipulated in the AMLO and AML/CFT Guideline. For the avoidance of doubt, AIs should also comply with applicable legal and regulatory requirements in their conduct of businesses.

[2] In the context of corporate, appropriate measures should be put in place to guard against the impersonation risk of the corporate's representative(s).

The AMLO and AML/CFT Guideline, which are in line with the international AML/CFT standards, provides flexibility for authorized institutions (AIs) to on-board corporate customers remotely. AIs may utilise various means to undertake CDD[3], including but not limited to, using third party intermediaries to conduct CDD on behalf of an AI; using an independent and appropriate person to certify identification documents; and using appropriate channels (e.g. teleconference or video conference), which are commensurate with the assessed money laundering and terrorist financing (ML/TF) risks, for customer interaction. Therefore, in the context of designing customer on-boarding processes, and under a risk-based approach, it is not necessary to ask a corporate's representative to visit the AI's business premise or to be physically present in front of a staff of the AI concerned in every case.

Technology is increasingly being used to enhance the process of on-boarding corporate customers; where used responsibly, it could help AIs manage risks more effectively and efficiently. For example, reliable technology solutions to verify the identities of individuals can also be used to facilitate the on-boarding of corporate customers through the verification of the identities of the corporate's representative(s) and beneficial owner(s)[4]. Whether or not technology is used in the CDD process, the regulatory expectation remains the same, that is, technology-neutral and risk-based. It means that processes adopted by AIs for remote on-boarding should be at least as robust as those performed when the customer is in front of the staff of an AI.

When designing on-boarding processes for corporates, including those conducted remotely, AIs should continue to differentiate the ML/TF risks of corporate customers in order to apply CDD measures and ongoing monitoring which are proportionate to the assessed ML/TF risks. The processes should reflect the principle that CDD is not merely a document collection exercise. To better understand the ML/TF risks and thus applying appropriate mitigating measures in the corporate segment, reference can be made to the Money Laundering and Terrorist Financing Risk Assessment Report for Hong Kong[5]. The report highlights ML/TF vulnerabilities associated with corporate vehicles, in Hong Kong as in other international business and financial centres, arising usually from complex or opaque ownership and control structures; cross-jurisdictional nature of many illicit transactions; and/or the inherent higher risks of products and services provided to corporates as compared to individuals.

---

[3] For the avoidance of doubt, depending on the circumstance, an AI may have to use a combination of means in order to complete all the CDD steps for a corporate customer on-boarded remotely.

[4] Reference can be made to the HKMA's circular on remote on-boarding of individual customers published on 1 February 2019. For example, iAM Smart, the digital identity being developed by the Hong Kong Government, is an acceptable technology solution for identity verification of individual customers.

[5] Published in April 2018, see paragraphs 4.37-4.41 for example. The report can be found at https://www.fstb.gov.hk/fsb/aml/en/risk-assessment.htm

The HKMA continues to work 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. AIs are encouraged to discuss with us any remote on-boarding proposals through HKMA Fintech Supervisory Sandbox 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)