Annex

Key observations and good practices in AML/CFT control measures for remote customer on-boarding initiatives

1. This note provides feedback from recent thematic reviews of remote on-boarding initiatives, insights and observations from our engagement with Authorized Institutions (AIs) and technology firms in the Fintech Supervisory Sandbox (FSS) and Chatroom as well as supervision of virtual banks. To provide greater clarity, specific high-level regulatory expectations are included in text boxes and supported by key observations and examples of good practices[1].

2. AIs should continuously review the effectiveness and efficiency of risk mitigating control measures implemented and refine such measures as appropriate. Reviews should take into account emerging threats and vulnerabilities relating to money laundering and terrorist financing (ML/TF), and ongoing assessment of the reliability and limitations of the technology solutions adopted in AIs' business-as-usual assurance processes, as well as key observations and good practices shared by the HKMA.

3. ***AIs should adequately assess ML/TF risks associated with a remote on-boarding initiative prior to its launch.***

3.1. All AIs reviewed had performed ML/TF risk assessments, with review and approval by Financial Crime Compliance (or equivalent) teams, before launching new initiatives. A number of AIs adopted a task force style approach comprising different front line departments and second line control functions to undertake the assessment. No particular format for the assessment is prescribed: for some AIs the ML/TF risk assessment was part of a wider scope assessment and more formal in nature, while others were in a standalone format. A number of AIs used an iterative approach to fine-tune risk assessments by seeking early supervisory feedback through the HKMA Fintech Supervisory Chatroom and testing results obtained through the FSS.

[1] AIs should note that these observations and examples are not meant to be an exhaustive list for meeting regulatory expectations.

3.2. Common factors covered in pre-implementation assessments included due diligence on the vendor's capability and the reliability of their solutions; possible impact and risks (including but not limited to ML/TF risk, impersonation risk) arising from remote on-boarding initiatives and technology used in the process; and any new or additional risks due to changes in AML/CFT control processes. The AIs reviewed adopted a risk-based approach to develop mitigating measures which were commensurate with the identified risks.

3.3. Some AIs that adopted off-the-shelf solutions for identity authentication and identity matching for remote on-boarding initiatives worked closely with the third-party vendor provider and as a result were able to demonstrate an appropriate level of understanding of how the solutions worked, for example both their benefits and limitations, including the algorithms used and the features / attributes matched by the artificial intelligence in the identity card authentication process. Such an understanding is essential for AIs adopting or planning to use remote on-boarding solutions. AIs that had a more limited knowledge of these features found the implementation process more complicated and were exposed to greater risk of the technology solution delivering unintended and inappropriate outcomes which could not be explained, leading to less effective overall management of associated risks. Some AIs had the ability to formulate their own test cases, by referencing different sources (e.g. threat intelligence) and research, to assess the reliability of the technology before and after launch.

4. ***AIs should apply a risk-based approach in the design and implementation of AML/CFT control measures for remote on-boarding initiatives.***

4.1. AIs should be able to demonstrate that the extent of customer due diligence (CDD) measures is commensurate with the ML/TF risks associated with a business relationship, irrespective of the means used to on-board a customer. AIs in the review recognised that remote on-boarding may involve ML/TF vulnerabilities which differ from some traditional processes (e.g. the scalability of fraudulent on-line applications). As a consequence, AIs in the review adopted a phased approach when launching remote on-boarding services, by initially targeting lower-risk customer segments and/or limiting the service scope (e.g. limited account functionality, lower transaction limits, restricting straight-through account opening).

4.2. Consistent with the risk-based approach, the control procedures for remote on-boarding applications varied according to the assessed risks. While some AIs do not currently on-board higher-risk customers remotely, others conduct part of the process through teleconference or video conference with applicants displaying some higher-risk characteristics to better understand and seek to manage the potential risks.

4.3. Some AIs adopted additional control measures, such as requiring first payments from same-name accounts at other banks to activate the account, to further mitigate impersonation risks. These AIs then incrementally expanded the customer segment and/or service scope based on operating experience and assessment of the effectiveness and efficiency of remote on-boarding processes.

5. ***AIs should monitor and manage the ability of the technology adopted to meet AML/CFT requirements on an ongoing basis.***

5.1. All AIs reviewed adopted ongoing quality assurance processes over the effectiveness of the end-to-end AML/CFT controls for remote on-boarding, including the technology deployed. Noting possible limitations in the pre-launch testing of the technology, all AIs reviewed were generally cautious in their initial approach in the light of new technology applied. For prudence sake, AIs generally applied 100% manual checking of selfie images, ID documents and liveness detection processes during the early stages of implementation to assess performance (e.g. false-acceptance rate and false-rejection rate) and identify any emerging risks (e.g. new ways to "deceive" the artificial intelligence embedded in the technology solution). AIs had also given consideration to the sustainability of 100% manual checking and planned to reduce the sample size over time taking into account the performance of the technology in terms of reliability and consistency, the availability and performance of other measures to mitigate the relevant ML/TF risks as well as supervisory feedback.

5.2. Some AIs undertook manual checks before the accounts were opened. AIs adopting a straight-through account opening process conducted manual checks after account opening and imposed some form of restriction until the checks were completed (such as limiting the amount of funds which could be transferred out) as additional risk mitigating measures. AIs would follow up any irregularities noted during manual checking and discuss adjustment or fine-tuning with vendors.

5.3. Apart from monitoring the effectiveness of the technology for remote on-boarding, manual checking is helpful for identifying any abnormalities and implementing appropriate risk mitigating measures or contingencies, for example where the artificial intelligence application does not perform as intended and cannot detect certain aspects such as unusual background of selfie or unusual facial expression by the applicant.

5.4. All AIs considered post-implementation reviews (PIR) after remote on-boarding initiatives were up and running as important to make sure that performance was as intended. Some AIs undertook this as part of an ongoing process while others undertook this as a standalone review, in which case the PIR was performed within a period of 6 to 12 month after implementation. Whatever form the PIR took, it was good practice to cover any new and/or emerging risks identified due to the adoption of the technology or changes to existing control processes.

6. ***Ongoing monitoring should take into account vulnerabilities associated with the product and delivery channel.***

6.1. The approach adopted by all AIs reflected the principle that CDD at on-boarding is only one part of effective AML/CFT controls. Since ML/TF risks will often only become apparent upon operation of the account, it is important to implement a monitoring system which is tailored to the risk profile of a customer relationship.

6.2. All AIs in the review were able to describe how CDD during on-boarding combined with ongoing monitoring to mitigate risks. While some AIs indicated they plan to apply specific rules-based detection scenarios to monitor transactions of customers on-boarded remotely, others are using or exploring different data points to monitor customer behaviour (e.g. data obtained for fraud prevention purposes).

6.3. We also noted some good practices in the regular sharing of information and intelligence. For example, some AIs established internal working groups with members from both Financial Crime Compliance (or equivalent) and anti-fraud teams to identify monitoring rules in the fraud monitoring system that had AML/CFT applications. In some cases, there were regular meetings to exchange information and conduct trend analysis and joint investigations of

ML-related fraud cases. Some AIs planned to adopt the same escalation flow and case management system to manage alerts generated from both the transaction monitoring and fraud prevention systems.