Annex

AML/CFT control measures applied by AIs in response to coronavirus disease (COVID-19)

The following examples are COVID-19 related interim measures applied by individual AIs specific to their own policies and procedures, which take into account not only the local legal and regulatory requirements, but also any group requirements and risk appetite. When making reference to these examples, AIs should carefully consider their specific circumstances and existing systems and controls. Relevant and adequate records, including any risk assessment performed, risk mitigating measures undertaken, and internal discussion and approval, should be maintained.

(I) Customer due diligence (CDD) under social distancing and travel restrictions

Customer on-boarding

1. Disruptions due to COVID-19 have affected the ability of AIs to use traditional methods to interact with customers, as well as the processes of physically verifying a customer's identity.

2. Remote on-boarding initiatives launched by AIs so far have been offered to individual retail customers. A few AIs, including some virtual banks, are expediting their plans to onboard corporate customers remotely leveraging on experience obtained and technology used for on-boarding individual retail customers. These initiatives are being or will be tested through the HKMA Fintech Supervisory Sandbox.

3. A number of AIs are using video conferencing as an interim measure to interact with customers during on-boarding and when undertaking ongoing CDD reviews. To mitigate any assessed risks, AIs using this approach have generally confined the service to a specific group of customers meeting certain criteria such as having business connections with other business segments, and applied additional control measures (e.g. the initial source of funds must come from same-name accounts maintained with other banks and no third party payment will be conducted before a face-to-face meeting is conducted).

4. Under the current exceptional circumstances, some AIs utilise the option of "delayed verification" as set out under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance for establishing new relationships where appropriate risk management policies and procedures are adopted. For example, some AIs accept scanned copies of identity documents from prospective overseas customers when establishing the business relationship as an interim measure, with physical identity documents being verified once this is possible. These AIs apply a range of measures to manage the risks involved when adopting this approach, such as limiting these interim measures to customers who were met by the bank staff prior to the COVID-19 situation; strengthening the monitoring of account activities; and limiting account functionality.

Ongoing customer due diligence

5. A number of AIs reflected that they had experienced delays in, or been unable to complete ongoing CDD reviews because customers were unavailable (e.g. unable to travel, quarantined or ill or unable to obtain required documents due to logistical challenges). Some AIs have made good use of the risk-based approach, for example, prioritising the review of higher-risk customers and seeking relevant approval for any exceptions made, generally for non-high risk customers. These AIs also maintained an adequate record of the relevant assessment and had a plan for clearing any backlogs as soon as possible.

6. Most retail banks have implemented some aspect of adverse news screening to support ongoing monitoring of customer relationships. One AI has temporarily lowered the priority of screening for lower-risk business segments to maintain adequate resources to manage higher-risk relationships or more critical functions; the AI concerned assessed the risks and based its decision on a risk-based approach as well as maintaining adequate records and staying agile to respond to any changes to its risk assessment.

(II) <u>Pressure on AML/CFT resources</u>

7. Most AIs are adopting work-from-home or split-team arrangements (e.g. split teams at different office locations on alternating schedules) as part of business continuity plans so as to maintain effective AML/CFT controls across their operations while minimising the infection risk. We have also seen efforts to reprioritise work on the basis of ML/TF risks to help relieve the pressure on resources.

Transaction monitoring and screening systems

8. The labour-intensive work of clearing alerts generated by transaction monitoring and screening systems has posed additional challenges to AIs during COVID-19, in particular, those relying on overseas service centres in heavily affected jurisdictions with lockdown measures imposed.

9. Some AIs moved quickly to meet this challenge by reprioritising alerts into different levels, to ensure a greater focus on the highest-risk alerts. Management reports are in place to closely monitor the situation together with a plan to clear the backlog cases as soon as the situation permits. Reallocation of staff, staggering office hours and suitably equipping staff to work from home have also helped to manage alert volumes in this period.

10. A number of AIs have also expedited the exploration of regulatory technology (RegTech) solutions (e.g. machine learning) to tackle the challenge of high false-positive rates, free up highly trained and experienced professionals to focus on genuine higher-risk cases and enhance the overall effectiveness and efficiency of transaction monitoring and screening systems.

11. Overall, AIs' responses have been categorised by the understanding that relevant controls or risk appetite should not be compromised when addressing operating issues.

(III) Emerging threats and changes in customers' behaviour

12. The HKMA drew AIs' attention to the report *"COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses"* published by the Financial Action Task Force on 4 May 2020 and AIs are aware of the increasing fraudulent activities and scam typologies associated with COVID-19.

13. Some AIs have observed an increase in digital payments and online transactions compared to normal levels as well as a rising trend of fraud cases. To continue to exercise vigilance in response to the changing risk areas for criminal activities, we noted that some AIs have provided specific guidance / reminders to staff to raise their awareness of fraud, scams and cyber security in relation to COVID-19. One AI has introduced additional mitigating measures based on risks, such as obtaining further information from customers or confirmation from correspondent banks before

processing transactions for accounts with specific features.

14. We are also seeing examples where the use of RegTech is helping to build out a more collaborative, intelligence-led approach to financial crime risk management and some AIs are applying advanced analytics to detect new threats, such as criminal networks and common vulnerabilities. For example, to understand a customer's global network, an international AI has launched a global analytics platform that identifies potential financial crime by analysing customer, transactional and publicly available data.

15. In response to the prevalent and emerging financial crime threats arising from COVID-19, industry-led initiatives have been established for the purposes of sharing good practices relating to prevention, detection and mitigation measures across the industry. Many AIs have reminded customers to stay alert of and not to fall victim to COVID-19 related scams or fraud, while some AIs have shared specific risk indicators and typologies with the industry in order to assist peer AIs to proactively identify accounts being used to receive fraudulent payments linked to COVID-19 and to undertake risk mitigating measures in a timely manner.