Annex

Risk Management Controls over Internet Banking Account Aggregation Service

1. Introduction

1.1 This Annex sets out the key principles and risk management controls that AIs are required to put in place when offering Account Aggregation Service to their customers.

1.2 Given the risks involved in implementing Account Aggregation Service, AIs should note that certain business models are, in principle, acceptable (see section 2) provided that adequate risk management controls (see sections 3 – 8) are put in place to address the associated risks while others are not allowed or only allowed subject to certain conditions due to the higher risks involved.

1.3 It is also important to note that, other than the risk management controls set out in this Annex, AIs should also implement other appropriate controls taking into account the relevant Supervisory Policy Manuals and circulars issued by the HKMA.

2. Acceptable Business Models

2.1 AIs should ensure that only the following types of bank accounts are allowed to be included in the service:

- for personal internet banking, AIs should only allow a customer to aggregate bank accounts that belong to him/her individually or jointly with other individual(s), in the case of an "either one to sign" joint account. For the avoidance of doubt, Account Aggregation Service involving joint accounts which require multiple signatories should not be allowed; and
- for business/corporate internet banking, AIs should only allow a business customer to aggregate bank accounts that are owned by the same company, the companies within the same group, or the same person/entity who has ownership in the companies (including joint venture companies). Proper authorisation such as a Board resolution should also be obtained from the relevant companies. If the business customers do not have any legal or affiliate relationship and apply for Account Aggregation Service, AIs should carefully assess whether there is a genuine and legitimate business purpose for the service and satisfy itself that the risk of the service being abused for conducting suspicious and illegal activities (e.g. money laundering) is low.

2.2 In addition, the service should only be provided by an AI in Hong Kong in co-operation with its affiliated banking institution(s), which include:

- its overseas[1] branch / head office; and
- its local or overseas subsidiary, affiliate or parent bank.

2.3 Providing the service in co-operation with unaffiliated institutions would involve more complex legal issues and is likely to expose AIs to a higher level of risk. AIs should therefore not provide Account Aggregation Service in these circumstances unless:

- there is no direct connection between the computer systems and networks of the institutions involved and data and instruction transmissions are via existing interbank financial messaging networks (e.g. SWIFT); and
- due diligence is conducted on the unaffiliated institution(s) involved and approval is obtained from senior management before establishing relationships with such institution(s) for the purpose of launching the service. The AI concerned should discuss its plan with the HKMA in advance and be able to demonstrate to the HKMA's satisfaction that such due diligence is conducted properly before implementing such an arrangement with an unaffiliated institution.

  For those AIs that have already established the service with unaffiliated institutions via interbank financial messaging networks, the AIs concerned should conduct proper due diligence as soon as possible to ensure that the existing arrangement is in compliance with all the regulatory requirements set out in this circular. Records and documentation of such due diligence should be made available to the HKMA if required.

2.4 In any case, AIs should not offer the service in co-operation with any entity that is not a banking institution.

3. Introduction of Account Aggregation Service

3.1 Similar to the launch of any new internet banking services as stipulated in the Supervisory Policy Manual on "Supervision of E-banking" (see section 2.3), an AI should discuss its plans with the HKMA in advance before launching, or making any major enhancements to Account Aggregation Service. In general, the discussion should satisfy the HKMA that the following issues are properly addressed:

---

[1] For the purpose of this letter, overseas entities also include entities in Mainland China.

- data privacy concerns (see section 4);
- legal and reputation risks (see section 5);
- technology-related issues (see section 6);
- money laundering concerns (see section 7); and
- consumer protection issues (see section 8).

4. Data Privacy Concerns

4.1 If Account Aggregation Service involves transfer of customers' personal data between local and overseas locations, it is important for AIs to disclose clearly and prominently to their customers the jurisdictions or locations where the data are transmitted and stored. The disclosure should be made when customers subscribe to the service or whenever such an arrangement is made. AIs should also ensure compliance with the applicable data privacy laws and regulations in local and overseas locations involved. For instance, AIs are required to comply with the provisions of the Personal Data (Privacy) Ordinance (PDPO) (particularly Data Protection Principle 3 & 4) in Hong Kong. In particular, if customers' personal data are required to be transferred to and/or maintained overseas, AIs should ensure that written consents are obtained from the customers involved and adequate security and controls are in place to safeguard such data.

5. Legal and Reputation Risks

5.1 As Account Aggregation Service may also involve collating bank accounts opened with overseas institutions onto an AI's internet banking website or vice versa, AIs should conduct proper due diligence (e.g. by obtaining proper and relevant legal advice and/or assessing the appropriateness of any legal advice provided by the relevant overseas institutions) to ensure that their proposed services comply with the related legal and regulatory requirements in the jurisdictions involved.

5.2 In particular, as Account Aggregation Service may involve funds being taken from a local bank account and deposited into an overseas account (i.e. cross-border fund transfer) under a common single sign-on operating platform (e.g. the local internet banking website of an AI), AIs should obtain appropriate legal advice to ensure that the proposed business model and service will not contravene the Banking Ordinance (BO), including among other things:

- section 12(1)[2] in respect of disallowing the carrying on of business of taking deposits in Hong Kong by any entity which is not an AI;

[2] According to section 12(1) of BO, no business of taking deposits shall be carried on in Hong Kong except by an authorized institution (other than an authorized institution the authorization of which is for the time being suspended under section 24 or 25).

- section 92 in respect of any advertisements posted on the internet for soliciting deposits from members of the public in Hong Kong;
- section 97 in relation to the use of banking name and section 97A in relation to the issuance of false statements as to authorized status; and
- section 46 in relation to the establishment or maintenance of a local representative office in Hong Kong by an overseas bank. One relevant consideration, among others, is whether the AI involved undertakes so much of the representative, liaison and/or promotional functions of the overseas institution that it has become an office of the overseas institution in Hong Kong.

5.3 In addition, AIs should also ensure that consent and/or approval from the relevant overseas authorities has been sought if this is a regulatory requirement set out by the relevant overseas authorities for launching the related service. Effective risk management controls should be implemented to ensure compliance with the legal and regulatory requirements in the jurisdictions involved.

5.4 As the AI and the other institution involved in Account Aggregation Service may be perceived by customers as connected parties, any problems (e.g. major information technology (IT) related fraud or system failure) occurring in the other institution will affect customer confidence as well as the reputation of the AI involved. AIs should therefore carefully assess the possible reputation risk before engaging other institutions in providing such a service.

6. Technology-related Issues

6.1 As Account Aggregation Service may involve a connection to be established or transmission of account information and instructions between the computer systems and networks of an AI and another institution, this will increase the security risk of the AI's computer environment. Such an arrangement will increase the number of access points to the AI's systems and the risk of intrusion to the AI's computer environment if the security controls of the other institution's internet banking system and/or the network connections between two entities are not adequate.

6.2 It is also important to note that certain supervisory requirements (e.g. two-factor authentication for high-risk internet banking transactions) issued by the HKMA may not have been implemented by the overseas institution as substantial differences may exist between jurisdictions with respect to internet banking supervisory requirements. As a result, fraudsters may take advantage of the less controlled systems of the other institution and gain unauthorised access to the AI's computer systems and customer accounts through this "back-door".

6.3 To address the potential technology-related risks, AIs should satisfy, among others, the following requirements:

- an independent assessment should be performed by an assessor with the necessary expertise[3] to confirm, before the launch of the service that the related systems and infrastructure implemented by the AI and the other institution are in compliance with the requirements stipulated in the relevant HKMA guidelines[4]. In particular, the level of security, internal controls, and contingency planning of the systems and infrastructure of the institutions involved should be at least equivalent to, if not more stringent than, those required by the HKMA. The AI involved should perform a formal risk assessment at least once a year, to determine if any further independent assessments are necessary and if so the frequency and scope of such independent assessments. The risk assessment should take into account, among other things, substantial changes to the risk profile of the services and significant modifications of the systems involved;
- effective controls should be established to ensure that customer data is kept confidential and will not be divulged to any person without the customer's consent. In particular, the AI's customer and transaction data should be properly segregated from the other institution and protected from unauthorised access by staff of the other institution. Access to customer data should be controlled by effective and adequate authentication mechanisms associated with proper access control rules.

7. Money Laundering Concerns

7.1 The provision of Account Aggregation Service may subject an AI to a higher risk of money laundering and terrorist financing, particularly if cross-border fund transfers can be conducted using this service platform. AIs should therefore carefully assess the related risks before introducing such a service and ensure compliance with the requirements set out by the HKMA[5] and other jurisdictions involved, on the prevention of money laundering and terrorist financing.

7.2 The controls in relation to the prevention of money laundering and terrorist financing should be reviewed from time to time in the light of the AI's experience in providing the service, taking into account any new or additional regulatory requirements

---

[3] See section 2.4.3 of the Supervisory Policy Manual on "Supervision of E-banking"

[4] The relevant HKMA supervisory requirements include, among others, Supervisory Policy Manuals on "General Principles for Technology Risk Management", "Supervision of E-banking", "Business Continuity Planning" and other related circulars issued by the HKMA.

[5] Including, among others, "Guideline on Prevention of Money Laudering", "Supplement to the Guideline on Prevention of Money Laudering" and other related circulars issued by the HKMA.

issued by the HKMA and other jurisdictions involved.

8. Consumer Protection

8.1 Due to the involvement of multiple parties (e.g. an AI and an overseas institution) in the provision of Account Aggregation Service, complications and uncertainties may arise in handling cross-border customer complaints, apportionment of liability and settlement of compensation claims for customers' financial loss arising from fraud cases and system failures, particularly for business models involving overseas or unaffiliated institutions. AIs should establish appropriate customer complaint handling procedures and internal guidelines for apportioning liability and settling any customers' claims for financial loss. Fair and balanced terms and conditions in relation to customer protection[6] should be included in the customer agreement for Account Aggregation Service. Appropriate legal advice should be sought in this regard when preparing customer agreements.

Hong Kong Monetary Authority
16 July 2010

[6] AIs should draw reference from the related guidance, among others, set out in the Code of Banking Practice and the Supervisory Policy Manual on "Complaint Handling Procedures".