A New Way for Overseas Individual Client Onboarding

On 28th June 2019, the SFC published a circular titled "Remote onboarding of overseas individual clients" (the "**Circular**") to provide a new guidance to intermediaries on remote onboarding of overseas individual client (the "**Client**"). Starting from 5th July 2019, the non-face-to-face account opening approach will be increased to five[1]; the new approach acceptable to the SFC is that intermediaries could onboard the Client via online. The regulatory requirements for new account opening approach are listed out hereinafter.

➢ Authentication of Identity Document

For the purpose of authentication of identity document of the Client, the following measures should be in place:-

(i) To (a) access the embedded data in the Client's official identification document (the "**ID Document**") (e.g. a biometric passport or an identity card); or (b) obtain electronic copy of the relevant sections of the ID Document;

(ii) To authenticate the ID Document by means of effective processes and technologies[2](e.g. check security features of the ID Document or verify the data obtained)[3] ; and

(iii) To follow the prescribed measures if third party is engaged to deal with account opening procedures involving the Client's personal information[4].

[1] (i) The signing of the client agreement and sighting of related identity documents certified by other persons (e.g. other licensed or registered person, a Justice of the Peace, branch manager of a bank, certified public accountant, lawyer, notary public or chartered secretary); (ii) Certification services recognized by the Electronic Transactions Ordinance (Cap. 553); (iii) The mailing of the completed and duly signed client agreement together with depositing a cheque in the sum of HK$10,000); (iv) Online onboarding of clients by using a designated bank account in Hong Kong; (v) Remote onboarding of overseas individual clients.

[2] The adopted technology should be thoroughly evaluated and tested by reference to international standards and best practices (e.g. ISO/IEC 19795 (Biometric performance testing and reporting) and ISO/IEC 30107 (Biometric presentation attack detection)).

[3] In case of a biometric passport, authentication may include scanning the data page, capturing data through optical character recognition and checking the captured data against the personal information stored in chip.

[4] When engaging a third party to carry out account opening procedures involving the Client's personal information, intermediaries should obtain the Client's prior consent and authorisation and put in place proper protection measures for security and confidentiality purpose.

➢ Verification of Client's Identity

In relation to verification of the Client's identity, the measures are set out as follows:-

(i) To match the Clients' biometric data obtained with the authenticated data in the ID Document[5]; and

(ii) To implement appropriate safeguards (e.g. data encryption and presentation attack detection[6]) to avoid potential presentation attack (e.g. video replay).

➢ Execution of Client Agreement

Intermediaries are required to obtain a client agreement signed by the Client by way of an "electronic signature"[7]. "Electronic signature" is different from "digital signature" and both of them are defined in the Electronic Transactions Ordinance (Cap. 553).

➢ Designated Overseas Bank Account

In addition, the Client must:-

(i) set up a bank account which is supervised by a banking regulator in an eligible jurisdiction[8] (the **"Designated Overseas Bank Account"**). Whilst the Designated Overseas Bank Account should be located in an eligible jurisdiction, the Client is not required to reside there;

---

[5] For example, intermediaries may capture the Client's facial image in real time and match it with photograph stored in the chip of the Client's biometric passport by using facial recognition technology.

[6] Presentation attack detection refers to the automated determination of a presentation attack (e.g. liveness detection).

[7] "Electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purposes of authenticating or approving the electronic record.

[8] As at 28th June 2019, there are 16 eligible jurisdictions, namely Australia, Austria, Belgium, Canada, Ireland, Israel, Italy, Malaysia, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, the United Kingdom and the United States of America but the 16 eligible jurisdictions do not include Mainland China. The SFC will update on their website the list of eligible jurisdictions in accordance with the results of the FATF's mutual evaluation.

(ii) transfer an initial deposit of not less than HK$10,000 or an equivalent amount in other currencies from the Designated Overseas Bank Account to the intermediary's bank account; and

(iii) any future deposits into and withdrawals from the Client's account with intermediaries shall only be conducted through the Designated Overseas Bank Account.

➢ Record Keeping

Intermediaries should maintain proper records for the Client's account opening process in a manner which is readily accessible for the purposes of compliance checking and auditing.

➢ Training

Staff responsible for onboarding the Clients should have received adequate training and should possess adequate knowledge and skills to implement and supervise the relevant procedures.

➢ Assessment

Intermediaries are required to retain a qualified assessor to evaluate and review the adopted processes and technologies prior to implementation and at least annually thereafter. The SFC is expected that such evaluation is performed by independent assessors.

➢ Senior Management Responsibilities

Senior Management including Managers-in-Charge are primarily responsible for ensuring that proper processes and technologies are implemented to verify the Client's identity.

➢ Domestic Regulatory Requirements

Intermediaries are reminded to comply with the requirements imposed by domestic regulatory authorities.

This explanatory summary is not, and should not be regarded as, a legal advice. Should you have any enquiries, please seek specific advice from legal advisers.

24th July 2019