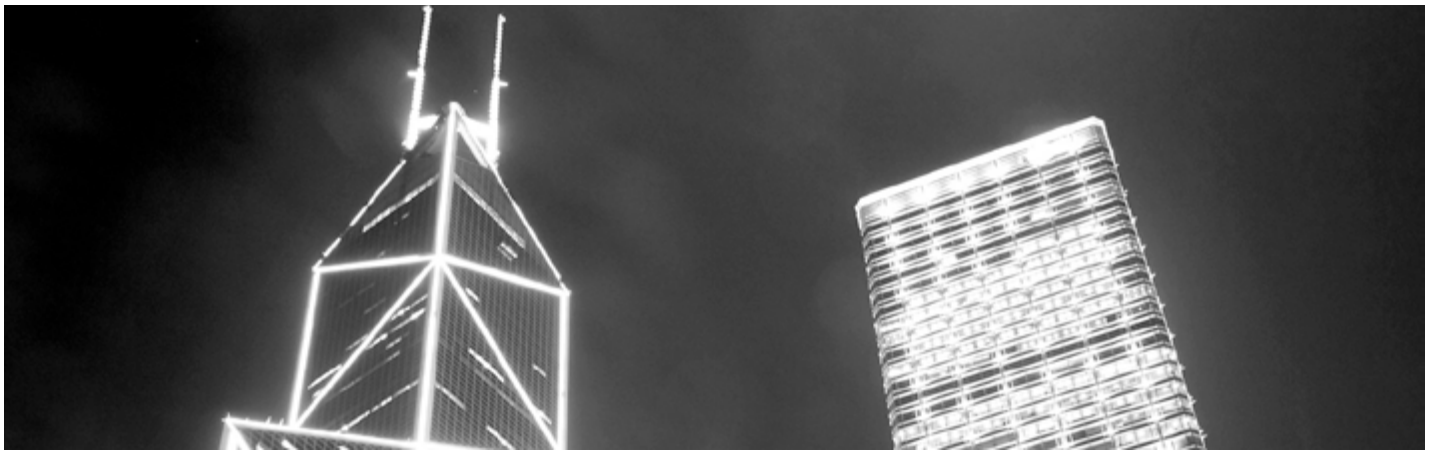
CHARLTONS
SOLICITORS



Hong Kong July 2019

Onboarding Clients Online: Changes to SFC's Code of Conduct Para 5.1

The remote onboarding of clients by SFC licensed intermediaries is facilitated by amendments to paragraph 5.1 of the Securities and Futures Commission's (**SFC**) Code of Conduct for Persons Licensed by or Registered with the SFC (**SFC Code of Conduct**) which took effect on 5 July 2019. Acceptable account opening methods are now set out on a designated SFC webpage at https://www.sfc.hk/web/EN/rules-and-standards/account-opening/,[1] rather than in the Code itself (see the SFC's "Circular to intermediaries: Amendments to paragraph 5.1 of the Code of Conduct"[2] of 28 June 2019). The SFC has given guidance on online onboarding of overseas individual clients in its "Circular to intermediaries: Remote onboarding of overseas individual clients",[3] also issued on 28 June 2019. The following provides a summary of the SFC's latest guidance on acceptable client account opening procedures.

Amendments to Paragraph 5.1 of the SFC Code of Conduct

Paragraph 5.1 of the SFC Code of Conduct sets out licensed intermediaries' Know Your Client obligations, requiring them to take all reasonable steps to establish the true and full identity of their clients. It previously contained specific guidance on acceptable methods of verifying clients' identity, which the revised paragraph 5.1[4] has deleted, referring instead to an SFC designated website (as referred to above) for acceptable account opening procedures.

New Designated Webpage

The new webpage has two sections:

1. Relevant regulatory requirements which include the SFC circulars and FAQs;[5] and

2. A description of what the SFC regards as acceptable account opening procedures.[6]

The SFC will update intermediaries in future as to other acceptable account opening procedures via circulars and publication on the designated website.

Acceptable account opening procedures

The acceptable account opening procedures described on the SFC's designated website are summarised below.

1 https://www.sfc.hk/web/EN/rules-and-standards/account-opening/
2 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC45
3 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC46
4 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/openAppendix?refNo=19EC45&appendix=0
5 https://www.sfc.hk/web/EN/faqs/intermediaries/supervision/account-opening/2019-06-28.html#2
6 https://www.sfc.hk/web/EN/rules-and-standards/account-opening/acceptable-account-opening-approaches.html

1. **Face-to-face account opening**

   Where accounts are opened face-to-face, the client must execute relevant documents in the presence of an employee of the licensed intermediary.

2. **Non-face-to-face account opening**

   a) Certification by other persons

   Where the client does not sign account opening documents in the presence of an employee of the licensed intermediary, signing of the client agreement and sighting of the client's identity documents should be certified by:

   i) any other licensed or registered person or an affiliate of a licensed or registered person which is a regulated financial institution;

   ii) a Justice of the Peace, or

   iii) a professional person such as a branch manager of a bank, certified public accountant, lawyer, notary public or chartered secretary.

   b) Certification services

   Certification services recognised by the Electronic Transactions Ordinance (Cap. 553) can be used (e.g., Hongkong Post's certification services).

   Certification services provided by overseas certification authorities whose electronic signature certificates have obtained mutual recognition status accepted by the HKSAR government can also be used for client identity verification. The latest Trust List of Certificate Types with Mutual Recognition Status is available at https://www.ogcio.gov.hk/en/our_work/business/mainland/cepa/mr_ecert/trust_list/hk_guangdong_ecert_trust.html.[7]

   c) Mail

   A licensed intermediary can verify individual clients' identity by following the procedure below:

   i) The new client sends the intermediary a signed physical copy of the client agreement with the client's identity document (identity card or relevant sections of the client's passport) for verification of the client's signature and identity;

   ii) The intermediary encashes a cheque for at least HK$10,000 obtained from the client and bearing the client's name shown on the relevant identity document. The cheque must be drawn on the client's account with a Hong Kong licensed bank;

   iii) The intermediary checks that the same signature appears on the client's cheque and the client agreement;

   iv) The client is informed of this account procedure and its conditions, including that the new account will not be activated until the cheque clears, either in the client agreement or by notice; and

   v) The intermediary keeps a record demonstrating that the client identification procedures have been followed.

   d) Online onboarding using a Hong Kong designated bank account

   Hong Kong clients can be onboarded online by the licensed intermediary:

   i) Obtaining a client agreement signed by the client using an electronic signature and a copy of the client's identity document, either an identity card or relevant passport sections;

   ii) Receiving a transfer to the intermediary's bank account of a deposit of at least HK$10,000 from the client's bank account with a Hong Kong licensed bank (**Designated Bank Account**);

   iii) Conducting all future deposits and withdrawals for the client's trading account only through the client's Designated Bank Account; and

7 https://www.ogcio.gov.hk/en/our_work/business/mainland/cepa/mr_ecert/trust_list/hk_guangdong_ecert_trust.html

iv) Keeping proper records of the account opening process for each client which must be readily accessible for compliance checking and audit.

Do previously acceptable approaches for new account opening still apply?

The SFC notes that all acceptable approaches for opening new accounts applicable prior to the June 2019 circulars are still acceptable.

Acceptable approaches for online onboarding of overseas individual clients

With effect from 5 July 2019, the acceptable procedures for remote onboarding of overseas individuals as clients are those set out in the "Circular to intermediaries: Remote onboarding of overseas individual clients",[8] which are summarised below.

1. **Identify document authentication**

   The following steps are accepted for verifying the identity of an overseas client:

   a) Either:

      i) access the data embedded in the client's official identification document such as a biometric passport or an identity card; or

      ii) obtain an electronic copy of the relevant sections of the identity document, including a high-quality photograph of the client.

   b) Authenticate the client's identity document using appropriate and effective processes and technologies. For example, check the security features of the identity document or verify data using a reliable, independent source. A biometric passport can be authenticated by scanning the data page, capturing data through optical character recognition and checking captured data against the client's personal information as stored in the passport chip.

   c) A client's prior consent and authorisation is required for a third party to carry out account opening procedures which involve the client's personal information. Licensed intermediaries must also put in place protection measures to ensure the security and confidentiality of clients' personal information.

2. **Identify verification**

   The client's biometric data should be obtained and matched with the authenticated data shown in the client's identity document. In obtaining biometric data, intermediaries must use appropriate and effective processes and technologies. The technology used should be thoroughly evaluated and tested, and reference may be made to international standards and best practices such as ISO/IEC 19795 (Biometric performance testing and reporting) and ISO/IEC 30107 (Biometric presentation attack detection). For example, intermediaries can use facial recognition technology to verify the client's identity by taking a photograph of the client and comparing it with the photograph stored in the chip in the client's passport.

   Licensed intermediaries must implement appropriate safeguards (such as data encryption and presentation attack detection) to protect clients' biometric data and the integrity of the identity verification process against potential presentation attacks.

3. **Client agreement execution**

   Obtain a client agreement signed by the client using electronic signature.

4. **Designated overseas bank accounts**

   An initial deposit of HK$10,000 should be transferred to the intermediary's bank account from the client's account with a bank which is supervised by a banking regulator in an eligible jurisdiction (a **Designated Overseas Bank Account**). The list of eligible jurisdictions is available on the SFC's website and currently includes the following 16 jurisdictions: Australia, Austria, Belgium, Canada, Ireland, Israel, Italy, Malaysia, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, the UK and the US.

8 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC46

All future deposits and withdrawals for the client's investments account must be made only through a Designated Overseas Bank Account.

5. **Record keeping**

Proper records must be kept for each client's account opening process which must be readily accessible for compliance checking and audits.

6. **Training**

Licensed intermediaries must ensure that staff responsible for online client onboarding have received adequate training and have the skills and knowledge to implement the procedures.

7. **Pre-implementation and annual assessments**

Licensed intermediaries should comprehensively assess client account opening processes and technologies prior to implementing them, and at least annually thereafter.

Pre-implementation assessment and annual reviews must be performed by qualified assessors with relevant knowledge and experience. The assessors for the pre-implementation assessment should also be independent of the licensed intermediary.

The minimum scope of the assessment and annual reviews is:

a) whether the processes and technologies used are appropriate and effective to establish clients' true identities, taking into consideration technological advances and the current sophistication of hacking and spoofing attacks;

b) whether the ongoing monitoring and review process (including reviews of identity document authentication and identity verification solutions) have been implemented appropriately and effectively;

c) whether the processes and technologies and all subsequent changes have been properly implemented and tested with satisfactory results; and

d) whether the requirements of sections 1-6 above have been followed properly.

An assessment report should be prepared for each assessment and review and submitted to the relevant regulator if requested. The assessment report's minimum required contents are:

a) a detailed description of the processes and technologies adopted;

b) details of the work performed, including an explanation of the scope and methodology of the assessment;

c) a confirmation that the adopted processes and technologies are appropriate and effective for establishing the true identities of clients and the basis and justification for the confirmation;

d) an explanation of the potential limitations (if any) of the assessment as well as the processes and technologies adopted. For instance, a discussion of the technologies adopted should cover:

i) the representativeness, quality and demographic diversity of the data used for developing and testing the technologies;

ii) the technologies' performance including the relevant parameters; and

iii) any material difference in the technologies' performance when handling client groups with different physical characteristics (e.g., age, gender and race);

e) recommendations for improvement (if any) of the adopted processes and technologies; and

f) management's responses to any assessor recommendations and, where appropriate, the status and timeframe for implementing any recommended steps.

In addition to performing pre-implementation assessments and annual reviews of technologies, intermediaries should also regularly evaluate the performance of adopted technologies to ensure that client identities have been properly established. Intermediaries

should immediately cease using a technology for client onboarding if it becomes vulnerable to a particular type of attack, and makes it difficult to satisfactorily verify clients' identities. They should only revert to using the technology once the intermediary is satisfied that the identified concerns have been addressed.

Responsibility for Verification of Client Identity

A licensed intermediary's senior management, including its Managers-in-Charge are primarily responsible for ensuring that proper processes and technologies are implemented to verify clients' identities.

CHARLTONS

Boutique Transactional Law Firm of the Year 2017
Asian Legal Business Awards

Hong Kong Office
Dominion Centre
12th Floor
43-59 Queen's Road East
Hong Kong
Tel: + (852) 2905 7888
Fax: + (852) 2854 9596

www.charltonslaw.com