Appendix 2

Key findings from the Exercise and the expected regulatory standards

The Exercise covered 12 small to medium-sized securities brokers. It was conducted by way of on-site inspections with the assistance of an external consultant, with a focus on the brokers' internal controls designed to protect client assets. Major deficiencies identified from the Exercise and the expected regulatory standards are summarised below. The measures and controls listed are not exhaustive. Each LC should review its own operations and specific circumstances to ensure that appropriate and effective control procedures are put in place and enforced.

1. Amendments to client particulars

a) System audit logs recording changes made to the client database were not regularly generated or reviewed by designated staff who were independent of those effecting the changes to detect any unauthorised alternations of client information.

b) Some LCs did not issue acknowledgement notifications to the clients' registered address, email or mobile phone when amendments were requested and made.

c) No checks were conducted on clients' new contact information against the client database to identify any common or similar patterns in correspondence addresses, email addresses and phone numbers that could indicate potential irregularities.

d) There was a lack of established procedures to verify clients' amendment requests sent via email by contacting them through their alternative contact information on the firm's official records.

Expected regulatory standards
e) LCs should handle requests to amend client particulars (including correspondence address, email address, phone number, designated bank accounts, authorised representatives) with due care to ensure that they are legitimate requests from the account holders. Appropriate measures should be implemented to verify the identities and signatures of the requestors and the legitimacy of the amendment requests. For example: i) The amendments are supported by written client authorisation[1]. LCs should conduct independent verification directly with clients at least on a reasonable sample basis[2] or when there is uncertainty about whether the requests are from a client, using the clients' alternative registered contact information in the firm's official records. This is

[1] Paragraph 3(b) of the Suggested Control Techniques and Procedures for Enhancing a Firm's Ability to Comply with the Securities and Futures (Client Securities) Rules and the Securities and Futures (Client Money) Rules (**Suggested Control Techniques and Procedures**) and point 2(b) of Appendix 2 to the "Circular to licensed corporations licensed for dealing in securities - Protecting client assets against internal misconduct" issued on 5 February 2016.

[2] Point 2(b) of Appendix 2 to the "Circular to licensed corporations licensed for dealing in securities - Protecting client assets against internal misconduct" issued on 5 February 2016.

essential even if the instructions seemingly bear the clients' signatures as they could be forged by fraudsters.

ii) When amendment requests are received and amendments are made, LCs should promptly issue acknowledgement notifications to the clients' registered address, email or mobile phone[3], which are not subject to change.

iii) LCs should stay alert to the requests for amending client particulars to identify and follow up on any anomalies[4]. For instance:

- the new email address has an unusual username or domain name, such as "mahjong123@domain.com" versus the original genuine email address "clientname@domain.com".
- the new bank account is maintained in a country that is not the client's usual residential or work location, even though it is in the client's name.
- the new correspondence addresses, email addresses or phone numbers are the same as or closely resemble those of other clients.

f) To prevent and detect unauthorised changes to client particulars, LCs should implement appropriate maker-checker controls for effecting changes in the client database[5], and designate an appropriate staff to regularly review the system audit logs which record changes made to the client database[6].

2. Handling of email requests

a) No formal guidance and regular training were provided to staff to raise their awareness of email scams and ensure that they understand the appropriate handling procedures.

b) Some LCs did not have written policies and procedures in place to manage the risks of email scams, including verifying the authenticity of email instructions received from clients.

Expected regulatory standards
c) LCs should implement policies and procedures to address the risks associated with accepting email requests for order placing, asset transfer or amendment of client

[3] The "Circular to licensed corporations - Managing the risks of business email compromise" issued on 24 March 2022 and point 9 of the self-assessment checklist attached to the "Circular to licensed corporations - Review of internal controls for the protection of client assets and supervision of account executives" issued on 19 December 2018.

[4] Point 1(h) of Appendix 2 to the "Circular to licensed corporations licensed for dealing in securities - Protecting client assets against internal misconduct" issued on 5 February 2016.

[5] Paragraph 7 of the Suggested Control Techniques and Procedures.

[6] Point 1(m) of Appendix 2 to the "Circular to licensed corporations licensed for dealing in securities - Protecting client assets against internal misconduct" issued on 5 February 2016.

particulars, as clients' email account might have been compromised and used by fraudsters to send fraudulent instructions[7].

d) Apart from verifying the requestors' email addresses against the firm's official records, LCs should have procedures in place to verify the authenticity of suspicious email instructions and email requests for order placing or asset transfer with amounts over a reasonable threshold, such as by confirming the instructions with clients using alternative registered client contact information, rather than responding directly to the email requests[8].

e) Sufficient guidance and regular training should be provided to staff to enhance their vigilance in identifying email scams and their understanding of the appropriate handling procedures[9].

3. Third-party deposits and payments and collection of physical scrips by third parties

a) Most LCs generally did not accept third-party deposits and payments except under rare circumstances. However, some LCs did not have written policies and procedures in place regarding the handling of third-party deposits and payments, particularly in relation to the specific circumstances under which such deposits and payments may be accepted, and the relevant control measures that should be adopted for accepting them.

b) An LC did not conduct independent confirmation with clients to verify the authenticity of stock withdrawals in physical scrips collected by third parties on the clients' behalf.

Expected regulatory standards

c) LCs should adopt a policy which discourages third-party deposits and payments and only accept them under exceptional and legitimate circumstances and when they are reasonably in line with the client's profile and normal commercial practices[10].

d) Where third-party deposits or payments may be permitted, LCs should implement policies and procedures to ensure compliance with the relevant regulatory requirements[11]. In particular, the policies and procedures should be approved by senior management and address, among others, the following:

- the exceptional and legitimate circumstances under which third-party deposits or payments may be accepted and their evaluation criteria;

---

7 The "Circular to licensed corporations - Managing the risks of business email compromise" issued on 24 March 2022.

8 The "Circular to all intermediaries - Beware of "Email Scam" " issued on 7 September 2012 and the "Circular to licensed corporations - Managing the risks of business email compromise" issued on 24 March 2022.

9 The "Circular to licensed corporations - Managing the risks of business email compromise" issued on 24 March 2022.

10 Paragraph 11.3 of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers) (**AML Guideline**).

11 Including Chapter 11 of AML Guideline, relevant circulars and frequently asked questions published by the SFC from time to time.

- the due diligence process for assessing whether third-party deposits or payments meet the evaluation criteria for acceptance; and

- the respective designated managers or staff members responsible for carrying out these policies and procedures[12].

e) Before client money and client securities withdrawals are made to third parties or physical scrips are collected by third parties on behalf of clients, LCs should independently verify with the clients the authenticity of the withdrawal requests, such as calling the clients on their registered phone numbers to confirm the withdrawals[13] and verifying the identities of the third parties who act on behalf of the clients against the clients' written authorisations[14].

4. Operation of bank accounts

a) Some LCs failed to implement proper authorised signer arrangements. For example, the firm's shareholders, directors or their nominees, who were not involved in the daily operations of the firm, were permitted to authorise payments from the firm's client bank accounts.

b) Some LCs allowed their staff to singly authorise payments out of the house and client bank accounts of the firms, while some LCs did not set authorisation limits for authorised signers to effect bank payments.

c) The rights of resigned staff were not removed from the list of authorised signatories in a timely manner.

d) Several staff were allowed to share a single user account for accessing the LC's online banking accounts.

e) Blank cheques were pre-signed by an authorised signer.

Expected regulatory standards

f) The SFC expects that the authorised signers of an LC for effecting any form of payments out of:

- the firm's client bank accounts should only be ROs, MICs or their delegates; and

- the firm's house bank accounts should be (i) ROs, MICs or their delegates, or (ii) any other persons provided that such persons can only effect payment jointly with ROs, MICs or their delegates[15].

12 Paragraph 11.3 of the AML Guideline.
13 Point 2(d) of Appendix 2 to the "Circular to licensed corporations licensed for dealing in securities - Protecting client assets against internal misconduct" issued on 5 February 2016.
14 Paragraph 2 of the Suggested Control Techniques and Procedures.
15 Paragraphs 10 and 11 of the "Circular to licensed corporations - Operation of bank accounts" issued on 28 June 2021.

g) LCs should consider requiring two or more authorised signers and setting appropriate authorisation limits for each of the authorised signers for effecting payments out of their house and client bank accounts, including online banking[16].

h) LCs should regularly review and update the authorised signer arrangements for the firms' bank accounts as well as the access rights to their online banking platform. This includes the timely removal of the rights of an authorised person who has left the firm or no longer holds the relevant role[17].

i) Each online banking user's access credentials (eg, passwords) and security device should be properly stored and should not be disclosed to another person, such that each user who has accessed the bank account and effected transactions can be uniquely identified, and unauthorised transactions can be detected[18].

j) Payment cheques to clients should be crossed[19] and under no circumstances are LCs' cheques to be signed unless the date, specified payee and amount portions of the cheques are properly filled in[20].

5. Dormant accounts

a) Some LCs failed to establish and implement written policies and procedures to periodically identify dormant accounts and regularly review the trading activities and other transactions in these accounts to identify irregularities.

b) Some LCs did not maintain any documentation of their reviews of the trading activities and asset movements in dormant accounts.

Expected regulatory standards

c) An account that has no trading activities and asset movements initiated by the account holder for a period of time, which should not exceed 24 months, should be classified as a dormant account.

d) Dormant accounts are susceptible to unauthorised dealing or other fraudulent activities. LCs should establish policies and procedures to regularly identify dormant accounts and review the trading activities and other transactions, if any, in these accounts to identify irregularities[21].

e) LCs should maintain proper records and documentation to demonstrate compliance with the expected standards for handling dormant accounts.

16 Paragraph 19 of Appendix to the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission (**Internal Control Guidelines**).
17 Paragraph 12 of the Suggested Control Techniques and Procedures.
18 Paragraph 15 of the "Circular to licensed corporations - Operation of bank accounts" issued on 28 June 2021.
19 Paragraph 14 of Appendix to the Internal Control Guidelines.
20 Paragraph 19 of Appendix to the Internal Control Guidelines.
21 Point 1(c) of Appendix 2 to the "Circular to licensed corporations licensed for dealing in securities - Protecting client assets against internal misconduct" issued on 5 February 2016.

6. Updates and maintenance of client information

a) For the circularisation exercise, about 8% of the total confirmation letters sent to clients' email or correspondence addresses were returned as undeliverable, suggesting that client contact information maintained in the LCs' official records was outdated.

b) An LC neither kept physical nor electronic copies of the account opening forms and specimen signature records for a portion of its clients in its office premises. Instead, these client documents were kept in an external warehouse, raising concerns about the ability of the LC and its staff to verify clients' signatures on written instructions during its day-to-day operation.

Expected regulatory standards
c) Updated client contact information enables clients to receive their trade documents timely and allows LCs to contact their clients promptly regarding urgent or important matters related to their accounts and the firm. LCs should establish controls to periodically review and update the records of client contact information in the client database to ensure that they are accurate and up-to-date[22]. Where there are undelivered contract notes and/or statements of account, LCs should follow up promptly with the clients to ensure that their contact details are accurate and up-to-date[23]. d) LCs should implement procedures to record and retain all relevant client information, related specimen signatures and supporting documentation[24]. They should ensure that this information is readily accessible to relevant staff for reference.

7. Segregation of duties

a) Some LCs allowed their dealing staff or AEs to handle client assets (including handling money and securities deposit and withdrawal requests from clients) as well as requests for amending client particulars, without implementing compensating controls.

b) Some LCs did not implement maker-checker controls for key operational functions. For instance, they granted both the input and authorisation rights to staff who could singly effect settlement instructions and physical scrip withdrawal instructions in the Central Clearing and Settlement System (**CCASS**).

[22] The "Circular to licensed corporations - Managing the risks of business email compromise" issued on 24 March 2022.
[23] Paragraph 7 of the Suggested Control Techniques and Procedures.
[24] Paragraph 1(a) of Appendix to the Internal Control Guidelines.

Expected regulatory standards
c) LCs should ensure that key duties and functions are appropriately segregated to minimise the potential for conflicts, errors or abuses[25]. Where complete segregation of duties is not feasible, LCs should assign duties in a way that ensures the necessary checks and balances are present and put in place adequate management review procedures over the key duties and functions to identify any error, abuse and fraud[26]. d) LCs should prohibit their front office staff (eg, dealing staff and AEs) from handling non-trade-related matters (eg, fund or stock deposit and withdrawal instructions and change of client particulars) unless there are compensating controls, such as arranging back-office staff (eg, settlement staff) to verify the instructions relayed by AEs with the clients directly[27]. e) Maker-checker controls should be put in place for key operational duties and functions, such as operation of the CCASS terminals and online banking portals. Appropriate limits for input or authorisation functions should be granted to each authorised person on a need-to-have basis[28].

8. System access controls

a) Some LCs did not appropriately grant system access rights to their staff on a need-to-have basis. For instance, some back-office staff were given access rights to front office systems to input and authorise trading orders, although these staff had never accessed these systems.

Expected regulatory standards
b) LCs should ensure that system access rights are granted to staff on a need-to-have basis only[29]. c) LCs should enforce physical access controls and information system security controls, such as log-in and amendment histories, to prevent and detect unauthorised access to or alterations of computer databases and circumvention of computer controls[30].

25 Part II of the Internal Control Guidelines.
26 The "Circular to licensed corporations - Guarding against risk of client asset misappropriation" issued on 1 February 2013.
27 Point 3(b) of Appendix 2 to the "Circular to licensed corporations licensed for dealing in securities - Protecting client assets against internal misconduct" issued on 5 February 2016.
28 Paragraph 16 of the Suggested Control Techniques and Procedures.
29 Paragraph 20 of Appendix to the Internal Control Guidelines and paragraph 11 of the Suggested Control Techniques and Procedures.
30 The "Circular to licensed corporations - Guarding against risk of client asset misappropriation" issued on 1 February 2013.

9. Reconciliation of client asset records

a) Some LCs failed to perform proper reconciliation between their ledgers and external records, such as bank statements and CCASS records. For instance, some LCs only performed client money reconciliation on a monthly basis, resulting in a breach of the Client Money Rules[31] by failing to properly segregate client money within one business day. Some LCs failed to do regular reconciliations for client securities kept in execution brokers.

b) Some LCs failed to timely and properly follow up discrepancies noted from the reconciliation process.

Expected regulatory standards

c) LCs should perform regular reconciliation of their internal records and reports to those issued by third parties (eg, clearing houses, banks, custodians, executing brokers, etc.)[32]. In particular:

- LCs should reconcile their internal stock records with the CCASS stock holding records on a daily basis. For stocks held in other locations, LCs should reconcile their stock records with those of third-party custodians at least on a monthly basis[33].
- On a daily basis, LCs should update their ledger accounts, reconcile the balances on client and bank ledger accounts and effect transfers to or from the client bank accounts in accordance with the Client Money Rules. In addition, they should reconcile their bank statements with their ledger accounts at least on a monthly basis[34].

d) All reconciliations of client asset records should be checked, reviewed and approved by appropriate senior staff members to ensure they are properly performed[35], and all discrepancies and outstanding items are properly and swiftly followed up[36].

31 Sections 4(4) and 10 of the Securities and Futures (Client Money) Rules (**Client Money Rules**).
32 Paragraph 10 of Part VII of the Internal Control Guidelines.
33 Paragraph 17 of the Suggested Control Techniques and Procedures.
34 Paragraphs 23 and 24 of the Suggested Control Techniques and Procedures.
35 Paragraph 10 of Part VII of the Internal Control Guidelines.
36 Point 1(a) of Appendix 2 to the "Circular to licensed corporations licensed for dealing in securities - Protecting client assets against internal misconduct" issued on 5 February 2016.