SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

6 June 2025

Circular to licensed corporations

Review of internal controls on client asset protection

The Securities and Futures Commission (**SFC**) issues this circular to highlight the red flags and control deficiencies found in certain asset misappropriation cases that licensed corporations (**LCs**) should remain vigilant about. It also shares key findings from its latest circularisation exercise on client accounts of selected small to medium-sized securities brokers and its review of these brokers' internal controls regarding client asset protection (collectively the "**Exercise**"), as well as sets forth the respective expected regulatory standards on LCs. Further details are provided in Appendices 1 and 2.

Client asset protection remains a top priority of the SFC. In this regard, the SFC has issued circulars[1] regularly to share its observations on control issues identified in its supervision work and provided guidance to LCs on the regulatory standards expected of them. However, the SFC has continued to receive reports from LCs and public complaints in recent years concerning misappropriation of client assets by fraudsters, including some dishonest staff of the LCs. Therefore, the SFC conducted the Exercise in 2024 with the assistance of an external consultant[2].

For some recent material cybersecurity incidents of LCs and phishing SMS messages received by clients of certain LCs, LCs should refer to separate guidance issued by the SFC regarding the standard of controls expected of them[3]. They should also remain attentive to other circulars and guidance published by the SFC from time to time.

Observations from the Exercise and reported asset misappropriation cases

The reported cases involved fraudsters impersonating LCs' clients to issue fraudulent instructions or LCs' staff gaining control of the firms' bank accounts to effect unauthorised payments. The red flags and control deficiencies of these cases are set out in Appendix 1, which include the following:

1. Fraudsters impersonated clients to issue counterfeit instructions by sending emails using email addresses which closely resembled legitimate ones of clients or hacking into clients' email accounts.

2. Fraudsters forged clients' signatures to issue counterfeit written instructions, which were sent to LCs by post, fax or email.

---

1 See the SFC's circulars dated 24 March 2022, 28 June 2021, 19 December 2018, 5 February 2016, 1 February 2013 and 7 September 2012.

2 See the "Circular to licensed corporations - Circularisation exercise and internal control review" dated 23 January 2024.

3 See the "Circular to licensed corporations - Cybersecurity review of licensed corporations" dated 6 February 2025, the "Circular to licensed corporations - Phishing detection and prevention" dated 21 May 2025 and the "Circular to licensed corporations - Prevention and handling of unauthorised trading incidents" dated 6 June 2025.

54/F, One Island East, 18 Westlands Road, Quarry Bay, Hong Kong
香港鰂魚涌華蘭路 18 號港島東中心 54 樓
+852 2231 1222 www.sfc.hk

3. These instructions usually involved:
   - amending client particulars, such as phone numbers, email addresses and correspondence addresses, in order to intercept clients' statements of account;
   - requesting LCs to execute transactions involving significant amounts of client assets;
   - transferring client securities to third-party securities accounts or withdrawing physical shares collected by third parties; and/or
   - transferring client money to third-party bank accounts or non-designated bank account purportedly opened in the clients' names but controlled by the fraudsters.

4. In a reported incident, a staff member was assigned both input and approval rights, enabling him to singly effect online bank payments from the firm's bank accounts to his personal bank accounts. In another case, some authorised signers failed to adequately safeguard their login passwords and the security tokens for the firm's online bank accounts, giving the dishonest staff a chance to steal them and execute unauthorised fund transfers.

Findings from the Exercise and the reported cases revealed deficiencies in LCs' internal controls regarding amendments to client particulars, handling of email requests and transactions involving third parties, and operation of bank accounts. The fraudsters and dishonest staff exploited these control deficiencies in LCs, not only jeopardising client interests but also causing significant financial losses to the LCs. Identification and monitoring of dormant client accounts are another area where controls should be tightened to mitigate the risk of unauthorised trading.

Details of the key findings from the Exercise and the corresponding expected regulatory standards on LCs are set out in Appendix 2.

Expected regulatory standards

LCs are reminded again of their obligation to put in place internal control procedures to protect their operations and clients from financial loss arising from theft, fraud and other dishonest acts[4]. They should implement adequate controls to protect client assets, especially in the following areas:

a) ***Amendments to client particulars:*** When amendment requests are received, LCs should ensure that they are from genuine clients by verifying the identities and signatures of the requestors. Verification should be conducted even if the instructions seemingly bear the clients' signatures which could be forged by fraudsters. Further, LCs should conduct independent verification with clients at least on a reasonable sample basis 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. In addition, when amendments are requested and made, LCs should promptly issue acknowledgment notifications to the clients' registered contact point which are not subject to change.

[4] Paragraph 4.3 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (**Code of Conduct**).

b) ***Handling of email requests:*** As clients' email accounts might have been compromised or hacked by fraudsters to send fraudulent instructions, LCs should implement policies and procedures to address the risks associated with accepting email instructions. Apart from verifying the requestors' email addresses against the firm's official records, LCs should take additional steps to verify the authenticity of suspicious email instructions and email requests for transactions with amounts over a reasonable threshold, such as by confirming the instructions with the clients using alternative registered client contact information, rather than responding directly to the email requests. Sufficient guidance and regular training should also be provided to staff to raise their awareness in identifying email scams.

c) ***Third-party deposits and payments and collection of physical scrips by third parties:*** As explained above, the SFC observes that asset misappropriation cases often involve third-party transactions, and such transactions carry higher risks for asset misappropriation, money laundering and other serious misconduct. Therefore, LCs should discourage third-party deposits and payments, and should only accept them under exceptional and legitimate circumstances with proper due diligence and management approval. Also, to prevent client asset misappropriation, before client money or client securities withdrawals are made to third parties or physical scrips are collected by third parties on behalf of clients, LCs should verify the authenticity of the requests by confirming directly with the clients and verify the identities of the third parties who act on behalf of the clients.

d) ***Operation of bank accounts:*** To prevent unauthorised bank payments, LCs should implement appropriate authorised signer arrangements and consider requiring two or more authorised signers for bank payments. Besides, authorised signers should not disclose their online banking user's access credentials to others and should securely store their security devices.

e) ***Dormant accounts:*** Dormant accounts are susceptible to unauthorised trading or other fraudulent activities. LCs should classify an account as a dormant account for close monitoring if there are no trading activities and asset movements initiated by the account holder for a period of time, which should not exceed 24 months.

Clients' awareness

Apart from the above, the SFC also wishes to remind LCs to take appropriate steps to raise their clients' awareness about protecting their interests. For example, LCs should regularly remind their clients to:

- properly safeguard their key personal information, such as specimen signatures, account login names and passwords, information about their investment and bank accounts, etc.;
- inform the firms of any changes in their personal particulars in a timely manner; and
- promptly check their trading documents including statements of account, and follow up with the LCs' management or independent staff instead of their account executives (**AEs**) in case of any discrepancies in their accounts.

Senior management responsibility

The SFC wishes to emphasise that senior management of LCs, including responsible officers (**ROs**) and Managers-In-Charge of Core Functions (**MICs**), bear primary responsibility for maintaining appropriate standards of conduct and implementing proper policies and procedures to adequately protect client assets and diligently supervise their staff[5].

The SFC is particularly concerned about some LCs' repeated control deficiencies in certain key areas, which cast doubts on their effectiveness in protecting client assets and call into question their fitness and properness to remain licensed. LCs should take all necessary steps to comply with the standards set out in this circular. If an LC repeatedly fails to put in place adequate and effective internal control systems which seriously jeopardise its clients' and the firm's interests, the SFC will not hesitate to take appropriate action against the LC and its senior management, including imposing conditions on the LC's licence[6] to manage or restrict the way it conducts regulated activities.

Should you have any queries regarding this circular, please contact your case officers or Ms Michelle Mak on 2231 1707.

Intermediaries Division
Securities and Futures Commission

Enclosures

SFO/IS/017/2025

5 General Principles 8 and 9 and paragraphs 4.2, 11.1 and 14.1 of the Code of Conduct.
6 Section 116(6) of the Securities and Futures Ordinance.