Appendix 1

Red flags and control deficiencies found in asset misappropriation cases

This appendix shares some examples of asset misappropriation cases reported by LCs or complainants, in which the LCs overlooked various red flags and control deficiencies. LCs are urged to consider the lessons learnt from these cases to raise their awareness of the threat of fraud on client accounts and internal misconduct.

1. Some fraudsters impersonated LCs' clients by using emails with either forged or compromised email addresses to issue instructions.

   (a) A fraudster emailed an instruction to an LC using a forged email address (contact@domainn.com) closely resembling that of a client (contact@domain.com) to add the fraudster as an authorised person to manage the client's account. Failing to identify the fraudulent email address, the LC approved the request. The fraudster then sent an email from the forged email address to instruct the LC to make a large payment to a third party arranged by the fraudster.

   (b) An LC received a fund withdrawal request via an email from a fraudster who had hacked a client's email account. The fraudster requested the LC to transfer a significant amount of the client's funds into a non-designated overseas bank account purportedly opened in the client's name but controlled by the fraudster. The LC processed the withdrawal request without confirming with the client directly and obtaining the client's written instructions to change the designated bank account as required by its internal policy.

2. Some fraudsters forged clients' signatures to issue counterfeit written instructions to LCs through postal mail, email or fax.

   (a) An LC received forged written instructions to change a client's email address for receiving account statements and to withdraw the client's securities of significant value in physical shares, which were to be collected by a third party arranged by the fraudster. The LC approved the requests without calling the client to verify the instructions.

   (b) An LC received a forged written instruction requesting to amend all contact information of a client, including the client's mobile phone number, email address and residential address. These changes prevented the client from receiving account statements. The fraudster then requested the LC to withdraw all of the client's funds to a non-designated bank account purportedly opened in the client's name but controlled by the fraudster. The bank was located in a country which was not the client's residential or work location.

   (c) An LC received a forged written instruction to alter a client's mobile phone number and email address. The LC's policy required its settlement staff to call the client to confirm the amendment request prior to making a change. However, the settlement staff conducted the confirmation by calling the new mobile phone number provided by the fraudster. The change in client particulars allowed the fraudster to reset and receive a new login password for accessing the client's online trading account to conduct unauthorised trades.

3. Control deficiencies in the operation of LCs' bank accounts could be exploited by dishonest staff.

   (a) An accounting staff of an LC was assigned with both the "input" and "approve" functions in the firm's internet banking portal such that he could solely effect payments. This enabled him to transfer the LC's house funds to his bank accounts without the knowledge of other personnel.

   (b) Two ROs of an LC were authorised to jointly effect online bank payments for both the firm's house and client bank accounts. However, they did not properly store their login credentials (i.e. the login names and passwords) and the security tokens. Their credentials and tokens were stolen by a staff member who then transferred a substantial amount of the LC's house funds and client funds into his bank accounts and disappeared.

Lessons learnt

4. When handling client instructions, LCs should diligently verify the instructions to ensure they are given by genuine clients. LCs should also stay alert to any instructions that deviate from the clients' normal practices, such as a client who usually provides online instructions suddenly sends written instructions by post.

5. LCs should raise staff awareness about the above red flags and control deficiencies when processing client instructions. They should also tighten up their internal policies and procedures and require their staff to strictly follow them in handling requests related to amendments of client particulars, withdrawals or transfers of client assets, and transactions involving third parties or bank accounts not designated by clients. In case of doubt, the responsible staff should always verify the instructions directly with the clients.

6. To prevent internal fraud, LCs should implement proper maker-checker controls for key operations such as online banking. User access credentials and security device should be securely stored to ensure the accountability of transactions effected and detect unauthorised transactions.

7. Please refer to Appendix 2 for more details of the expected regulatory standards on LCs in the above areas.