Circular

24 March 2022

## Circular to licensed corporations

## Managing the risks of business email compromise

The Securities and Futures Commission (SFC) has recently received reports from licensed corporations (LCs) about business email compromise, a type of cyber fraud whereby fraudsters posing as known business contacts dupe unwary staff into sending them money or sensitive information. These incidents resulted in the leakage of client information which undermined client interests and, in some cases, significant financial losses which the LCs had to bear.

### Business email compromise

A business email compromise (BEC) scheme typically involves one or more of the following actions by the fraudsters[1]:

- forging an email address which looks like that of a genuine client contact for communicating with the target LC[2];
- impersonating client contacts and making apparently legitimate requests such as asking for copies of statement of accounts, adding or altering authorised signatories, applying for user accounts or placing trade orders; and
- issuing fund transfer instructions, usually to bank accounts under their control at multiple receiving banks, some of which are located overseas, to maximise their chances of receiving the funds.

In most cases where fraudsters succeeded, the identities of the email senders were either not verified or were checked improperly. For example, an LC staff simply called the phone number provided by the fraudster and followed the confirmation to process the fund transfer instructions.

In addition, many red flags were ignored by the LCs. In one incident, fund transfers were rejected or withheld by some banks. Instead of promptly investigating the irregularities, the LC proceeded to act on the transfer instructions to other banks. Eventually, a number of fund transfers were effected, inflicting financial losses on the LC.

LCs should take note of the examples of BEC provided in the Annex.

### The SFC's expectations

The SFC expects LCs to have internal control procedures and financial and operational capabilities which can be reasonably expected to protect their operations and clients from financial losses arising from theft, fraud and other dishonest acts, professional misconduct or

[1] Besides impersonating clients, fraudsters might also pose as other business contacts, such as vendors or suppliers, to request payment.

[2] A forged email address may have a similar domain name (eg, xyzz.com instead of xyz.com) or a slightly different username but the same domain name (eg, abcc@xyz.com instead of abc@xyz.com).

omissions[3]. LCs are reminded to vigilantly monitor and effectively manage BEC risks, especially at times when remote working arrangements are commonplace[4].

*Control mechanisms*

LCs should establish effective policies and procedures to provide guidance to their staff for managing BEC risks. In addition, LCs should strengthen internal controls in the following aspects:

*Client contact information*

- Establish true identities of the clients and their authorised representatives during the account opening process.
- Periodically review and update the official records to keep client contact information accurate and up-to-date.

*Amendment of client particulars*

- Request written instructions when a client asks to amend his or her particulars (including updating authorised representatives)[5], and verify the requestor's identity and specimen signature.
- Verify email requests using contact information on LCs' official records, rather than the email address or phone number provided in the email. Consider arranging a video conference or a physical meeting with the client if needed.
- Issue acknowledgement notifications to the clients' registered address, email or mobile phone when amendments are requested and when they are made.

*Email requests for order placing or fund transfer*

- Implement effective confirmation procedures for the requests with the amounts over a reasonable threshold.
- Rather than responding directly to email requests, use alternative channels and contact information from LC's original records to contact and verify client's requests.
- Consider using surveillance tools to filter spoofed email addresses and detect unauthorised access to internal networks and systems.

---

[3] Paragraph 4.3 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission.
[4] Circular to LCs on management of cybersecurity risks associated with remote office arrangements dated 29 April 2020.
[5] 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.

*Red flags*

- Stay alert and handle with extra care when email requests are inconsistent with the client's normal practices. Promptly follow up irregularities, such as significant payments to overseas bank accounts, requests for immediate payments and repeated transfer rejections by banks.

- Foster a strong risk culture to encourage staff to report and follow up on red flags. Engage supervisors, IT administrators and compliance staff in a timely manner to formulate appropriate responses to suspicious email instructions.

**Senior management responsibility**

It should be noted that the above control measures and techniques are by no means exhaustive. The SFC suggests that each LC review its own circumstances and ensure that appropriate and effective control procedures are put in place and effectively enforced. It is the responsibility of the senior management to oversee LCs' implementation of internal control policies and procedures for the effective management of BEC risks, and ensure that adequate resources for such control functions are allocated and proper checks and balances are in place.

LCs should provide regular training to staff to enhance their vigilance in watching out for email scams and ensure that they understand the appropriate handling procedures. LCs' staff should carefully examine email addresses, prudently verify the authenticity of requests, diligently investigate red flags and promptly escalate issues according to internal protocols.

LCs are also advised to make reference to the SFC's guidance on the control measures and techniques for managing cybersecurity risks[6] and guarding against email scams[7].

Should you have any queries regarding the contents of this circular, please contact your case officer.

Intermediaries Supervision Department
Intermediaries Division
Securities and Futures Commission

End

SFO/IS/019/2022

[6] Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading published on 27 Oct 2017.
[7] Circular to All Intermediaries: Beware of "Email Scam" dated 7 Sep 2012.