Examples of business email compromise (BEC)

This annex shares some examples of BEC attacks targeting licensed corporations (LCs). LCs are encouraged to consider the lessons learnt from these examples to raise their awareness of BEC threats.

Case 1

Broker A received multiple emails from "fundd@domain1.com", posing as its client (fund@domain1.com), and instructing it to sell the client's stocks and transfer the sales proceeds to unregistered offshore bank accounts.

Broker A executed the instructions but neither enquired about the non-designated bank accounts nor investigated the obvious red flags when banks rejected the first few transfers. Subsequent transfers were accepted by other banks, resulting in a significant loss. The scam was discovered when the client questioned the unauthorised trades and fund withdrawals.

Although Broker A's senior management were alerted to the repeated bank rejections, they did not take any action. LCs should promptly follow up on red flags and senior management should exercise adequate supervision over the business activities of their firms.

Case 2

A fraudster impersonating a corporate client (contact@domain2.com) sent an email via "contact@domain22.com" to Broker B to request statements of account. After receiving the documents, the fraudster sent a signed application form to add himself as a new authorised signatory. Broker B did not discover the unauthorised signatory and incorrect entity name on the form, and approved the addition request.

The fraudster then made an urgent payment request via email by providing a forged letter of authorisation. Broker B called the fraudster on the phone number provided in the email to verify the instruction and processed the payment. The scam was discovered when the fraudulent email address was spotted in an email which also copied Broker B's genuine client contacts.

LCs should diligently verify email instructions received to ensure that the sender is a genuine existing client and his/her instructions are properly authorised. Moreover, LCs should perform effective verification of email instructions based on their own registered contact or bank account information.

Case 3

Broker C received several fund withdrawal requests to transfer several million dollars to various overseas bank accounts from "cllientw@domain3.com", which resembled a registered email address of its corporate client (clientw@domain3.com).

A staff member at Broker C attempted to verify the instructions with the client, but the phone number on record was uncontactable. Becoming aware of the different email address, he also asked the sender to confirm using the registered email account. However, the fraudster had taken control of the client's email account and was able to use it to send an email confirmation to Broker C's staff, who processed the withdrawals. The scam was discovered when the client enquired about the unauthorised transfers.

LCs should ensure that clients' registered contact information is accurate and up-to-date for timely verification. Furthermore, LCs should be alert to the possibility that fraudsters may have taken control of clients' registered email addresses and should verify instructions via reliable alternative channels.

Case 4

A fraudster used an email similar to that of a third-party vendor to request payment from Broker D. Staff failed to notice the unusual email address and to verify whether bank account details are the same as the vendor's bank account for settling payment. The LC transferred several million dollars to the fraudster's account. The fraud was later discovered by a staff member who noticed that his email account was hacked.

LCs should be aware that, apart from posing as clients, fraudsters might also impersonate other business contacts, such as vendors or suppliers, to request payment. LCs should act quickly to address hacking risks when they become aware of any suspicious emails or unusual activity in their email accounts.