HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

March 20, 2018

Dispute Resolution

Overview of Cross-border E-mail Fraud and Asset Recovery in China

Andy LIAO | Shirley LIAO

With the wide use of e-mail in the ordinary course of business, hackers increasingly enter e-mail systems to deceive users and defraud them of money or property. This kind of fraud is particularly prevalent in cross-border transactions which, including payment processing, are heavily reliant upon e-mails due to time zones and language barriers. These circumstances provide an opportune chance for hackers to plot their crimes. The most common e-mail fraud is a type of phishing scam, whereby hackers send out payment instructions by using e-mail addresses that are identical or nearly identical to those of staff working for trading companies or senior executives of multinationals. For this reason, it is also known as “trade fraud” or “CEO fraud.” When a company discovers it has fallen victim to the fraud, it is often quite helpless because it is difficult for the judicial authorities or financial institutions to discover the fraud and immediately freeze the funds as the funds have been transferred to banks in different jurisdictions and the hackers usually use shell companies to receive funds.

Han Kun’s commercial dispute resolution team has represented many multinationals to handle a significant number of cases relating to e-mail fraud and asset collection in recent years and we have accumulated a wealth of practical experience as a result. This article intends to provide an overview of the main types and methods of e-mail fraud, major remedies victims may seek, and the relevant legal and practical issues involved. Considering that the particularities of each individual case impact the selection of specific strategies, a successful asset recovery requires timely involvement and efficient handling from experienced counsel who are familiar with local judicial process.

E-mail Fraud

a. Main Types of E-mail Fraud

Main Types	Common Fraud Scenarios	Discovering the Fraud
Trade Fraud	Trading company A is negotiating sales of goods with its foreign client B, when the parties are close to a deal, the hacker impersonates A and sends an e-mail to B: (1) "The goods have been exported, our original bank account is under audit and cannot receive new funds, please pay to the following account of our Hong Kong subsidiary..."; (2) "We are negotiating and resolving tax issues with our bank, please make the payment to our affiliate company as follows… ".	Trading company A has still not yet received the payment after a long time and decides to send another e-mail or call B directly, both parties are shocked to discover the wrongful remittance.
CEO Fraud	The hacker impersonates senior executive A and sends an e-mail with the subject "Urgent and Confidential M&A" to financial staff B: "I am currently on a business trip in China conducting a highly confidential M&A deal, please pay attorney fees/consulting fees to the following Chinese company immediately and do not to tell any other third person regarding the e-mail and purpose of the payment."	When the senior executive A appears in front of B or B goes through payment formalities with A, they are shocked to discover the fraud.

b. Carrying Out the E-mail Fraud

i. Confirming the Target

Hackers gather contact e-mails of trading companies or multinationals through their websites or foreign business forums. Free corporate e-mails with poor security protection or personal e-mails without unified corporate suffixes are more likely to be targeted. Hackers hack into the targeted e-mail accounts and intercept e-mail correspondence between the parties or steal the password of and log into the targeted e-mail account to learn of the transaction progress.

ii. Secret Observation

Instead of acting immediately, hackers usually take time to review all related e-mails to familiarize themselves with internal corporate structure, financial procedures, senior executives' agenda, transaction progress, and even to imitate writing styles of the parties, all of which lay the foundation for the contemplated phishing e-mail at the key point of payment.

iii. Phishing E-mails

At the key point of the wire transfer, hackers cut off e-mail communications between the parties and impersonate the trading company to request a change of bank account or impersonate the senior executive to request the financial staff to execute a wire transfer.

The phishing e-mail is rarely sent from the actual e-mail address being targeted, the prevalent form of the fraud is to use a forged e-mail address that merely resembles the actual e-mail address. To lower the suspicions of the victim, hackers usually use the forged e-mail address to intervene at an earlier stage before payment in normal communications between the parties, such as exchanging documents or checking on transaction progress. Below are examples of common means to forge e-mail addresses:

Methods	True e-mail address	Forged e-mail address
Character resemblance	apple@qq.com	app1e@qq.com
Increase or decrease in character count	sasaki@sahathai.com	sasaki@sahatthai.com
Suffix replacement	vicky@yahoo.com	vicky@ymail.com

iv. Money Laundering

Hackers often cash out immediately or after several transfers after the funds have been wired, but their whereabouts are at risk of being exposed. It is thus common at present for hackers to launder the funds through a second transaction. Specifically, before hackers send out the phishing e-mail to foreign clients requesting a change of bank account, they will negotiate with another trading company for a purchase of goods and request the trading company to provide their bank account and to export the goods upon receipt of the payment. The bank account provided by the trading company will be designated as the false account in the phishing e-mail. Thus, the hackers are not only able to resell the goods received, but also to launder the illegal funds and make the case harder to solve and the funds more difficult to trace.

Asset Tracing and Recovery Strategies and Methods

Upon discovering the e-mail fraud, it is a top priority for the victim to contact the banks involved and the police immediately to freeze the funds or to disclose the movement of the funds. For a foreign remitter, efforts should immediately be made to contact its bank to cancel the transfer. Even if the transfer has been executed, the remitting bank is in a more advantageous position than its client to find the proper persons in the receiving bank and to lobby them to restrict or delay further transfers, especially when the banks cooperate on the money laundering and so on.

It is noted that local police in China, when receiving a report from a foreign victim, are inclined

to reject the case on the grounds that they lack the jurisdiction or the reporting documents are incomplete, and advise the foreign victim to report the crime to local law enforcement in their home country or to Interpol, which will result in missing the best opportunity to recover funds. The receiving bank faces a dilemma in these fraud cases; although it is sympathetic to the victim, due to the contractual duties of confidentiality to its clients and indeterminacy of the case, it usually states it has no right to take measures against the suspected account before receiving any instructions or orders from judicial authorities. Given this, it is vital for the victim to engage local counsel to provide practical assistance for case acceptance and asset freezing in preparing reporting materials, arranging and translating evidence, and providing explanatory documents to local police and the receiving bank to address the jurisdiction issue and bank regulatory provisions.

A successful fund freezing certainly buys sufficient time for the next step of asset recovery, the major options are set out as follows:

a. Local Criminal Investigation and Prosecution or International Police Cooperation

When the funds are successfully frozen or the hackers are located where the receiving bank is situated, a local police investigation is undoubtedly the most efficient way to apprehend the criminal suspects and recover the assets. Even if the funds have been transferred, an investigation will be helpful to trace the movement of the funds and take the next steps. We previously assisted a client to cause the local police to order the receiving bank to disclose information about where the funds were transferred, and our client used this fund transfer information to trace the funds to a bank account held by a Hong Kong company. Through cooperation with Hong Kong counsel, we successfully caused the Hong Kong police to take investigative measures against that company and its senior executives.

For such kind of cross-border fraud, it is theoretically possible to resort to Interpol. The remitter may report the case to the National Central Bureau of Interpol located in its home country, which will then transfer the case to the receiving bank's National Central Bureau with a request to take action. However, Interpol tends to focus on high profile cases and does not publicize working procedures. It is difficult for the victims to maintain efficient contact with Interpol or predict the outcome of their cases. Therefore, fraud victims normally will not utilize the Interpol approach as the sole remedy and will also report the case to the local police concurrently.

b. Civil Litigation

The opportunity to apprehend hackers or to recover funds is not very optimistic due to the use of high technology and cross-border complications. Victims usually resort to civil litigation if they cannot recover the funds through the police. Generally, there are the following options in practice:

i. The Foreign Remitter Files Suit against the Recipient based on Unjust Enrichment

The recipient normally dares not to or cannot appear before the court if the recipient is a hacker or a hacker-controlled shell company. Unjust enrichment claims filed by the foreign remitter will basically be upheld by the courts as the recipient will fail to provide legitimate reasons for the receipt of funds.

Laundering of the funds, however, will complicate the case. The foreign remitter is at risk of losing the case if a trade relationship or a consignment collection is established between the recipient and the hackers. Unjust enrichment means profits are acquired without a legal basis by one party and cause losses to the other party. In this scenario, the recipient normally will respond proactively by arguing they have a contractual basis to receive the funds, such as sales of goods or consignment collection. According to our experience and observations, the result of a judgment will mainly depend on the evidence presented by both parties.

ii. The Foreign Remitter Files Suit against the Receiving Bank based on Property Damages

Filing suit against the recipient is unproductive if the receiving bank is controlled by the hacker and the funds have already been transferred. Considering that the hackers may use false identity documents to open the account, we note that some foreign remitters have filed suit against the receiving bank to request compensation based on the bank's negligence in reviewing and verifying the applicant's identity documents. According to our observations, the results of these judgments are inconsistent because courts hold different opinions as to whether the review should be substantial or not and how broad the scope of the review should be.

c. Diplomatic Channels

Most countries set up police liaison offices in their embassies abroad to promote information exchange and law enforcement between their countries and the local police relating to trans-national crimes. Consulates normally play a role in promoting and protecting their overseas trade and investment in China. Therefore, it may be productive for victims or their lawyers to seek protection from the embassy or consulates. The local police will be more receptive and may take proactive steps upon receiving a diplomatic note from an embassy or consulate.

Conclusion

E-mail fraud is on the rise in recent years with scams that are similar in design and implementation as those described in this article. Trading companies and multinationals should take precautionary measures by safeguarding their e-mail and network systems. If a case of e-mail fraud occurs, it is a top priority to take immediate measures to secure the funds and then to recover the funds through police, judicial, diplomatic and other routes.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact **Mr. Andy Liao (+86-21-6080 0990; andy.liao@hankunlaw.com).**