DORSEY™
always ahead

GUIDE TO PROTECTING AGAINST EMAIL WIRE FRAUD SCAMS AND RECOVERING FUNDS WIRED TO HONG KONG

By Steven Nelson and Janet Wong

Background

There has been a recent dramatic increase in email wire fraud scams (also known as "**Business Email Compromise Scams**" or "**BEC scams**") perpetrated against companies worldwide whereby funds are wired to fraudsters' bank accounts in Hong Kong.

The FBI reports that the majority of the fraudulent transfers are wired to Asian banks located within Hong Kong and mainland China. The FBI has also published statistics regarding the large scale of the problem.[1] For example, from October 2013 through February 2016, law enforcement received reports from 17,642 victims resulting in US$2.3 billion in losses, and a 270 percent increase in identified victims and exposed loss since January 2015.[2] These figures probably understate the dimensions of the problem.

Hong Kong, in particular, is facing a multimillion-dollar email scam crisis. Hundreds of victims are scammed each year, with the average amount by which they are defrauded increasing by more than a third in 2015 from 2014.[3] The BEC scams are occurring at an alarming rate and even large sophisticated companies are falling victim. The scams occur when a business executive's or employee's email account is compromised or spoofed. The fraudster is able to steal money with the help of an unwitting accomplice, usually an employee who is fooled into submitting a wire transfer of funds to an international bank account.

Quick and decisive action is required as soon as the fraud is detected. This guide sets out how to help minimise the risk of falling victim to such scams and what to do in case you have been defrauded by a BEC scam.

How are the scams perpetrated?

The scammers are sophisticated and go to great lengths to hack, spoof and mimic company email addresses and email signatures or use social engineering techniques to assume the identity of a CEO, a company attorney or trusted vendor. They research company employees who manage money, falsify documents specific to the company they are targeting and even adopt the style of writing that would be expected of the assumed identity to make their emails as convincing as possible. Gone are the days of the obvious warning signs of criminal activity, such as bad grammar and spelling, or unrealistic scenarios.

The scammers will try to compromise an employee's email account to see what they can learn and will also check publicly available information such as the company's webpage, press releases and social media. They are looking out for general information about the company, where it does its business and with whom, names and titles of company officers, management organisational structure, who reports to who and so on.

After someone within a company has been deceived into believing that they are communicating with a legitimate and known person, the scam may continue over a period of days or weeks including back and forth emails and may even include telephone calls. The fraud is typically executed by requesting an urgent wire transfer using dollar amounts that lend legitimacy.

A common technique scammers adopt is to send emails that appear authentic on their face. They are crafted to give the impression that they have been sent by someone the recipient has had previous dealings and communications with, but are in fact sent by someone assuming an identity known by the fraud victim. These scams hinge on an email request that appears completely legitimate, either coming from an actual email account or one that is so similar that all but the closest scrutiny would miss the variation. If the scammers have not been able to compromise an executive's email account, they create a look-alike domain (a "spoofed email domain"). For example, the scammer may use an email address that is identical to the legitimate email address as well as the same email signature of the sender, but change it by either adding a hyphen or underscore, add a country extension to the email address domain such as johnsmith@fraud.com compared to johnsmith@fraud.com.au or making changes that are difficult to detect without careful scrutiny, such as substituting the letters "ri" for "n".

1 See FBI Public Service Announcement dated 27 August 2015 at https://www.ic3.gov/media/2015/150827-1.aspx.

2 See https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams

3 It has been reported that HK$605 million was defrauded from 489 victims due to BEC scams in the first six months of 2015, compared to HK$983 million across 1,095 companies for the whole of 2014. See http://www.scmp.com/news/hong-kong/law-crime/article/1870341/email-scammers-strike-again-hong-kong-company-loses-hk18m

Emails may also be hacked and hijacked. The scams often involve scammers infiltrating the IT system of the target through an email or internet based Trojan horse or malware that allows them to view email communications. This allows the scammers to use information to help them deceive their target. Scammers often target companies that pay their invoices by wire transfer. By viewing email communications of the target, they often wait for a legitimate party to send an invoice, and follow it up with a scam email (assuming the identity of the legitimate party) with new fraudulent banking instructions.

There are various versions of the scams and victims range from large corporations to tech companies to small businesses to non-profit organisations. Many times, scammers target businesses that work with foreign suppliers and those that regularly perform wire transfer payments. Often, scammers direct funds to be wired to company bank accounts in Hong Kong or mainland China.

What to do in case you have been defrauded by a BEC scam

As soon as funds are transferred to a scammer's bank account, they will attempt to transfer/withdraw as much of the deposited money as quickly as they can, often to other overseas accounts making recovery extremely difficult. Therefore, as soon as you become aware that you have been victimised by a BEC scam, you should immediately:

- contact your bank and request that they contact the financial institution where the fraudulent transfer was sent and seek an immediate hold or reversal of the transfer; and
- file a police report in the jurisdiction to which the money was transferred as soon as possible. [4]

In addition to the above, you should engage the help of lawyers located in the jurisdiction to which the money was transferred as soon as possible to help liaise with local police and file urgent civil proceedings to freeze the recipient account and thus prevent any onward transfer of the funds.

Insurance protection

It is also worth checking your insurance policies to see whether you are insured against fraud, theft or dishonesty. In terms of coverage availability, many policies preclude coverage if the funds are transferred voluntarily (even if through deception). However, recently, insurers have developed a product that would address BEC scams. The coverage is known as Social Engineering coverage, which must be added by endorsement to a standalone policy. Limits tend to be low, with high deductibles and numerous protocols in place in order for insurers to agree to provide coverage.

How to help minimise the risk of falling victim to a BEC scam

To detect potential BEC scams, it is necessary to look holistically at the requested wire transfer details, how and when the request was submitted, and the relationship between the originator and beneficiary. The following indicators should raise a red flag for potential BEC scams:

- transfer amounts that are unusual (higher or lower) for a particular business account or vendor;
- payments to beneficiaries that are new or are outside of where the business typically operates. For example, a first time request for a wire transfer to a bank account in China or Hong Kong;
- changes in established payment practices such as frequency and timing; and
- email-only wire transfer requests and requests involving urgency.

In addition, the following practices will help minimise the risk of falling victim to a BEC scam:

- increasing awareness within an organisation (especially those authorising wire transfers) of the existence of BEC scams;
- verifying legitimate business partners and new payment instructions in person or by telephone to a previously known or independently verified telephone number and not to a number provided in the email;
- being cautious of spoofed/mimicked email addresses;
- practising multi-level authentication;
- implementing technology solutions to identify suspicious emails by, for example, scanning hardware for any spyware, malware, Trojan horses etc. that may be able to spy on the Company's IT system, and establishing a program or warning system that will raise a red flag if the name on an incoming email does not exactly match an existing contact.

4 If you are in the United States, you may also file a complaint with the Internet Crime Complaint Center (IC3), but such filing will have limited benefit if the funds have been wired internationally.

How we can help

We have assisted numerous clients in their attempts to freeze and retrieve money lost due to wire fraud. The key to successful recovery upon discovering a fraud is to act as soon as possible to freeze the funds in the recipient bank account.

As noted above, it is common for BEC scams to transfer defrauded funds into bank accounts in Hong Kong, where the absence of foreign exchange controls means that funds can be credited promptly to the destination account and then easily transferred into mainland China. Given prompt notice, we can act on behalf of a victim to file a report with the Hong Kong police and notify the recipient bank. With the filing of a police report, the police may inform Hong Kong's Joint Financial Intelligence Unit, which may issue a "no consent" letter to the bank involved, putting the bank on notice of a suspicious transaction. The bank is not required to take any action upon receipt of a no consent letter, but will generally freeze the suspect account to avoid the risk of violating Hong Kong's draconian anti-money laundering legislation.[5]5

The police will then liaise with the bank to inform it of the suspect transaction and may get a sense of how much money remains in the account. However, the details of the bank account opening and transaction history will not be disclosed in the absence of a discovery order issued by Hong Kong courts, which will reveal such information.

Unfortunately, Hong Kong police will not assist with the recovery of defrauded funds, at least where there is no evidence that either the victim or the fraudster is in Hong Kong. It may take some time for the police to investigate the fraud and there is no guarantee that the bank will voluntarily freeze the account. Therefore, the next step is to bring urgent civil proceedings in the Hong Kong courts against the persons holding or having an interest in the funds sought to be recovered. If there are any funds left, in order to retrieve them, we generally seek an urgent ex-parte injunction order to freeze the bank account. This will ensure that funds can no longer be accessed by the fraudsters. It may also be necessary to obtain a discovery order to ascertain how much money is left in the account and the details of any subsequent transfers.

At the same time, we will file a claim for the defrauded funds and seek judgment on the same, without which the banks generally will not release any funds that are retained in the account. In most instances, judgment will be by default, and a garnishee order may be required to be served on the bank before any funds are released.

It may take between 4 to 6 months before any funds are retrieved out of court proceedings depending on the complexity of the case and any interlocutory matters.

Steven C. Nelson
Dorsey & Whitney
50 South Sixth Street, Suite 1500
Minneapolis, MN 55402-1498
(612) 340-2942
nelson.steve@dorsey.com

Janet Wong
Dorsey & Whitney LLP
88 Queensway
Suite 3008, One Pacific Place
Hong Kong
(852) 2105-0266
wong.janet@dorsey.com

5 Section 25A(2)(a) of the Organised and Serious Crimes Ordinance, Cap 455 and the "no consent" regime does not operate to withhold or freeze the accounts or property of a suspect. It only creates a defence for further dealings with the property after disclosure. It remains for financial institutions to decide whether to honour the instructions of their customers despite their suspicion and the disclosure.