Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How To Protect Against Business Email Compromise Scams

Law360, New York (January 12, 2016, 1:21 PM ET) --


Robert Pé


Winson S. Chu


Suzanne Siu

Over the last two years, the FBI has reported close to 10,000 businesses victimized by a particular form of online fraud referred to as a business email compromise scam or BEC scam, which typically involves the fraudulent transfer of funds from the company to accounts in Hong Kong and mainland China. According to the FBI, more than 8,000 businesses fell victim to business email compromise scams and suffered a combined loss of more than $1.2 billion.[1] Since January 2015 there has been a 270 percent increase in the number of victims falling victim to BEC scams and a similar increase in the total amount of loss they suffered. The FBI reported that in the majority of BEC scams the funds are transferred to bank accounts in Hong Kong or mainland China.

U.S. Department of Homeland Security agents contacted the authors of this article after we had successfully frozen the proceeds of a BEC scam in bank accounts in Hong Kong. The DHS is particularly concerned about the apparent ease with which fraudsters have been able to gain control of bank accounts in Hong Kong, notwithstanding the theoretically stringent anti-money laundering procedures in place.

What is a BEC Scam?

The BEC scam relies on the use of an email account that has been "hacked" or "spoofed." The most common type of email sent by a fraudster to initiate a BEC scam is an email that appears to be from (i) a supplier asking the business to settle an invoice by wiring funds to a specified account, (ii) a senior executive (e.g., CEO or CFO) within the business asking the employee to arrange a wire transfer and/or (iii) an external lawyer asking the employee to arrange a wire transfer in connection with a corporate transaction. Recent variations of the BEC scam have involved an employee receiving both an internal email and an external email — for example, an internal email from a senior executive asking the employee to assist a lawyer with a corporate transaction, followed by an external email from the said

lawyer requesting a wire transfer.

Fraudsters will often conduct research regarding the business and use such information to make their emails appear legitimate. For example, fraudsters may use the identity of a genuine supplier or lawyer or they may describe actual transactions under negotiation.

The email sent by the fraudsters appears authentic on its face — it may originate from (i) a legitimate email account that the fraudster has hacked, (ii) an email address that is very slightly different from a legitimate email address, or (iii) an email address that is identical to a legitimate email address but the reply is directed to a different email address.

Case Study — Part 1

Below, we set out a case study based on a real life matter.

The financial controller of a U.S. company received an email purporting to come from the CEO of the company. It indicated that a named external counsel would contact the controller in connection with a planned acquisition, asked him to do as requested by the counsel, and indicated that the controller should contact the CEO if at any stage he had any questions. The scam depended on the controller and the CEO being in different locations and not bumping into each other in the office corridor — something which the fraudsters had almost certainly researched. Likewise, the controller was not surprised to receive the email because he had heard mention in the past few weeks of plans for the company to do an acquisition — something of which the fraudsters were probably aware.

The name given for the "counsel" was that of a real-life transactional lawyer with a mid-size U.K. commercial and private client law firm.

How to Avoid Becoming the Victim of a BEC Scam

Increased awareness of BEC scams, additional scrutiny of wire transfer requests and good internal communications will help protect a business against such a scam. Finance departments should establish clear procedures for verification of wire transfer requests, including both internal and external requests. For example, finance departments should:

- Record the agreed/usual payment process and bank account details of suppliers and other counterparties;
- Ensure that all wire transfer requests and invoices are consistent with the agreed/usual payment process and that the bank account details match up; and
- Verify thoroughly any wire transfer request that involves a new counterparty, payment process or bank account.

Any unusual wire transfer request should be verified both internally and with the external counterparty, either in person or by telephone call to a previously known or independently verified telephone number and not to a number provided in the email.

IT departments should implement measures to identify suspicious emails. For example, they should

configure the email server to flag such emails.

Case Study — Part 2

A person purporting to be the external counsel contacted the financial controller while he was enjoying a day off. The "counsel" explained that he was acting for the company in connection with a major acquisition and that because of U.S. Securities and Exchange Commission regulations it was critical to maintain confidentiality. If at any stage the controller had questions or concerns, he should email the counsel or the CEO. The counsel indicated that he would need the controller's assistance in arranging a series of wire transfers. The first of these had to be arranged urgently that day.

The fraudsters almost certainly knew that the controller would be taking a day off and working only on a mobile device. This, in turn, meant that he would be less likely to follow standard procedures and more willing to comply with the apparently important and urgent request.

The controller made calls and sent emails to his office to arrange the first wire transfer. Over the next 48 hours the "counsel" made multiple calls and sent multiple emails to the controller who arranged two further wire transfers. The three wire transfers, for a total amount of $12 million, all went to bank accounts in Hong Kong, one account in the name of a Hong Kong company and the other in the name of a British Virgin Islands company.

The "counsel" requested a fourth transfer for $80 million. When the controller indicated that he was uncertain whether the company had sufficient cash reserves available, the "counsel" indicated that, if necessary, the company would have to draw down on its credit facilities. At this point the controller became nervous, called the CEO and realized that he had been scammed.

What to Do When You Fall Victim to a BEC Scam

When a business suspects that it has fallen victim to a BEC scam, it should immediately:

- Contact the bank from which it made the wire transfer(s) and ask the bank to freeze or reverse the transfer(s) — for this purpose, it is important to have the contact details of several individuals at the bank. It is ideal if those individuals are located in different time zones so that the business can reach someone at the bank outside normal office hours; and

- Urgently obtain legal advice on making a report to the law enforcement agencies and on locating and recovering the funds — given the international nature of these scams, it will usually make sense to engage an international law firm.

In doing all of the above, it is important not to alert the fraudsters to the fact that their scam has been uncovered.

As indicated above, in many BEC scams the funds are transferred to bank accounts in Hong Kong. If this happens, you should urgently obtain legal advice on making a report to Hong Kong's Joint Financial Intelligence Unit (JFIU). The report to the JFIU can be done online and the process is quick and straightforward.[2] The JFIU will often be able to freeze funds in the recipient bank account. However, it

will not generally be at liberty to disclose information regarding the action, if any, it has taken.

Businesses will often need to rely on civil proceedings to locate, freeze and recover funds transferred to a bank account in Hong Kong as the result of a BEC scam. This will frequently involve making a court application for (a) a Mareva injunction against the recipient of the funds, freezing its relevant bank account up to the amount of the funds transferred, and (b) Norwich Pharmacal relief (pre-action discovery) to obtain bank records and other documents from the recipient bank. The bank records may reveal that the funds have been transferred to other banks accounts. If so, further applications for Mareva injunctions and Norwich Pharmacal relief may be needed.

In making such applications, it is important to keep in mind:

- The application for a freezing order will be made ex-parte without the intended defendant present. This is to avoid alerting him and affording him an opportunity to dissipate the funds. As a result, the applicant will be under a strict "duty of full and frank disclosure" and must disclose all material facts, whether helpful or harmful to its case. If it fails to comply with this duty, the freezing order is likely to be discharged later;

- The applicant for a freezing order will have to provide a "cross-undertaking as to damages" that the intended defendant may suffer and will sometimes have to "fortify" its cross-undertaking with a payment into court or bank guarantee. If the freezing order is granted and is subsequently found not to have been justified, the applicant will have to compensate for any loss or damage suffered;

- Giving notice to the recipient bank of a freezing order and effecting service quickly and effectively will be critical, as will ensuring that the bank complies promptly with the order. This will require advance preparation in terms of identifying relevant contacts at the bank and obtaining their contact details; and

- An application for pre-action discovery will require the applicant to provide an undertaking to reimburse the recipient bank's costs of locating and copying relevant documents. It is important quickly to build a collaborative relationship with the bank.

The victim can sue for the recovery of the funds but may face competing claims. For example, the current holder of the funds may claim to have received them as payment for goods or services delivered. Alternatively or additionally, other victims of the same fraudsters may come forward and assert that their money has been mixed with the funds identified and frozen. It is important to be aware of such issues at an early stage and to move quickly and decisively.

Case Study — Part 3

After the financial controller realized he had been scammed, the company immediately reported the matter to its bank in the U.S., which contacted the recipient bank in Hong Kong and asked it to freeze the funds received as a result of the wire transfer. The Hong Kong bank was broadly cooperative but

would not provide firm confirmation of the status of the funds. The company also reported the matter to the local police force where it was headquartered and to the FBI, which alerted the Hong Kong authorities.

The company commenced civil proceedings in Hong Kong for the recovery of the wire transfers. The Hong Kong court granted an injunction to freeze the recipient account on the grounds that the company had a strong arguable claim, there were assets in the jurisdiction (in the form of the funds in the account), there was a real risk of those assets being dissipated and the balance of convenience lay in favor of granting the company the injunctive relief sought.

The Hong Kong court also granted an order requiring the recipient bank to disclose relevant bank records, including records to show where the money had subsequently been transferred. As a result, the company was able to trace the money into another bank account and to obtain an injunction freezing that further account. The company eventually recovered all three wire transfers that it had paid out.

—By Robert Pé, Winson S. Chu and Suzanne Siu, Gibson Dunn & Crutcher LLP

Robert Pé is a partner in Gibson Dunn's Hong Kong office. Winson Chu and Suzanne Siu are associates in Gibson Dunn's Hong Kong office.

[1] http://www.ic3.gov/media/2015/150827-1.aspx

[2] See http://www.jfiu.gov.hk/en/str.html