

Protecting Against Business Email Scams and Recovering Funds Wired to the United States

by Janet Wong and Steven C. Nelson

Background

“Business Email Compromise Scams” or “BEC scams” typically target companies that conduct wire transfers with entities abroad. For example, a fraudster may use an email address that is very similar to that of a business’s actual vendor to request payment for invoices, with payment to be wired to a bank account that the fraudster controls in another country. In this way, the fraudster fools an unwitting employee into assisting with a theft of funds that, after being sent, are very difficult to recover.

Over the years, there has been significant reporting about BEC scams that see funds wired to fraudsters’ accounts *in Hong Kong or mainland China*. But, we have seen a recent surge of BEC scams against businesses in mainland China or Hong Kong with funds being sent *to the United States*.

In the event of a BEC scam, decisive action is required as soon as the cyber fraud is detected. This guide describes what to do if you are victimised by a BEC scam with money being wired to the United States and how to help minimise the risk of falling victim to BEC scams to begin with.

How are the scams perpetrated?

Typically, wire fraud scammers research company employees who manage money and determine with whom a company does business. Often, scammers infiltrate a victim’s IT system through an email or internet-based Trojan horse or malware that allows them to view the victim’s email communications. This lets scammers observe payment requests from legitimate business partners and identify key personnel.

Armed with this information, fraudsters impersonate business partners, commonly sending emails that appear on their face to have originated with such partners. For example, fraudsters may use an email address that is identical to a legitimate email address, but for a small change, like an added hyphen. With such manipulated email

Related People

- Janet Wong
- Steven C. Nelson

Related Capabilities

- Financial Services Regulatory
- Privacy & Social Media
- Asia-Pacific
- China

addresses, scammers send what appears to be standard requests for payment, often in the form of authentic-looking invoices. Typically, these requests direct that a wire transfer be sent to a foreign bank account that the business partner has never used.

How to reduce the risk of falling victim to a BEC wire fraud scam

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

- a request to transfer amounts that are unusual (higher or lower) for a particular business;
- a request to transfer funds to beneficiaries that are unknown or outside of a business partner's typical area of operation. For example, a first-time request for a wire transfer to be sent to a bank account in the United States warrants closer inspection;
- changes in established payment practices such as frequency and timing; and
- email-only wire transfer requests, particularly requests asking for urgent action.

More broadly, the following general practices will help reduce the risk of being victimised by a BEC wire fraud scam:

- increasing awareness within an organisation of the existence of BEC scams;
- verifying payment instructions in person or by telephone to a known or independently verified telephone number – not to a number provided in an email request for payment;
- carefully reviewing email addresses to detect spoofed/mimicked email addresses;
- employing multi-level authentication; and
- implementing technology solutions to identify suspicious emails by, for example, scanning hardware for any spyware, malware, Trojan horses, etc., and establishing a program to warn if the name on an incoming email does not exactly match an existing contact.

What to do if you have been defrauded by a BEC scam

Scammers typically withdraw funds immediately after those funds hit a scammer-controlled account, including by sending funds to yet another account or converting them to cryptocurrency. Obviously, this makes recovery quite 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 it communicate with the financial institution to which the fraudulent transfer was sent in the United States to seek an immediate hold or reversal of the transfer; and
- retain an experienced wire fraud lawyer in the United States to liaise with the U.S.-based recipient bank and with U.S. law enforcement, and potentially to file an emergency civil proceeding to freeze the recipient account.

Insurance protection

It is also worth checking your insurance policies to see whether you are insured against fraud, theft or dishonesty. 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 stand-alone policy. Limits tend to be low, with high deductibles and numerous protocols in place in order for insurers to agree to provide coverage.

How Dorsey can help

Dorsey has wire fraud lawyers in Hong Kong and the U.S. who have assisted numerous clients in attempting to freeze and retrieve money lost due to BEC scams. The key to successful recovery upon discovering a fraud is to act as soon as possible and to leverage existing relationships with banks and authorities.

When funds are transferred to the U.S., it is essential to have a U.S. attorney who is able to contact the recipient bank and U.S. law enforcement immediately. Such immediate contacts are typically only possible if the U.S. attorney has pre-existing relationships with a wide range of banks and U.S. law enforcement – as Dorsey does. Through such existing contacts, follow-up requests to freeze funds can be made. In addition, information can be gathered regarding the actual beneficiary of the transferee account, the amount of any funds remaining in an account, secondary recipients of funds, and the nature of the criminal scheme at issue. These facts are typically critical in persuading law enforcement to pursue perpetrators and to determining how best to seek recovery of funds, including through potential litigation.

To be clear, Dorsey assists clients in filing formal reports with law enforcement and making formal inquiries of recipient banks. But such reports and inquiries often do not produce quick action, and, in connection with BEC scams, quick action is essential. Thus, while formal post-theft inquiries are important, the ability to reach immediately law enforcement agents or recipient bank personnel is essential.

Our experienced U.S. and Hong Kong wire fraud lawyers have handled numerous cross-border wire fraud cases and are well-equipped to provide expert assistance and guidance. Please visit our **[International Cyber Crime and Asset Recovery](#)** page.

Our specific articles include:

- **[Recent Trends in Wire Fraud Scams: Uncovering and Tackling the Latest Tactics in Hong Kong](#)**
- **[Guide to Protecting Against Email Wire Fraud Scams and Recovering Funds Wired to Hong Kong](#)**
- **[Hong Kong Email Wire Fraud Epidemic](#)**
- **[Hong Kong and Overseas Businesses Defrauded of over HK\\$1.8 billion \(US\\$231m\) in 2016](#)**

Contact one of our wire fraud lawyers for further assistance and guidance in tackling cross-border wire fraud cases.

Joshua Colangelo-Bryan, Of Counsel

Janet Wong, Partner

Steven Nelson, Senior Partner