LOCKE LORD® QUICKStudy
November 4, 2014
Business Litigation & Dispute Resolution Practice

Wire Transfer Email Fraud and What You Can Do About It

By: Greg Burch, Adrian Taylor and Christie Yeung

Businesses are increasingly falling prey to a clever email-based fraud that does not use sophisticated hacking techniques. Take a few simple steps to increase your company's security, and if money is stolen you may be able to recover it if you act quickly.

How The Fraud Works

People envision computer crime as either highly technical hacking or unsophisticated email come-ons like the infamous Nigerian money scam emails. But an increasingly common kind of fraud lies in between, and relies on clever deceptions, "social engineering" and careful use of publicly available information that companies readily publish on their websites. This kind of fraud depends on use of a real email address that is deceptively similar to one that would be used by the target company or its legitimate suppliers to trigger a kind of "fictitious payee" scam. The target company is tricked into sending funds by wire transfer to a bank account under the fraudsters' control. This bank account is often in Hong Kong, and the timeframe for intercepting and recovering funds that have been stolen in this way is very short.

Three Basic Elements To The Scam

1. Fraudsters secure an internet domain name that is visually very similar to the domain name of the target company or of the target's real suppliers. For instance, if the target company is named USA101, Inc. and its domain is www.usa101.com, the fraudsters will secure registration of www.usa1001.com.
2. Scammers will research publicly available information about the target company looking for the names of senior financial officers and employees, especially chief financial officers and comptrollers.
3. Fraudsters will use what hackers call "social engineering" to secure the name and legitimate email address of a target company employee who is responsible for making large wire transfers. This last is usually done with one or two simple telephone calls: "Hi, I'm Fred Jones from ABC Bank. I need to send an email to whoever just sent us a wire transfer for $625,000. Can you give me that person's name and email address?" It is fairly common that fraudsters can secure a name and email address over the phone in this way with very few attempts.

With that last piece of information, the fraudsters have two vital parts of the scam: the name and email address of a person who is authorized to initiate wire-transfers, and the format of legitimate company email addresses. If the name of the person with wire transfer authority is Sandy Smith and her email address in our example is SSmith@usa101.com, and they learn from the company's website that the CFO's name is Roger Black, they will know that the CFO's legitimate email address will very likely be RBlack@usa101.com. Putting all these pieces together can take experienced fraudsters just a few hours of work.

The next step in the scam is sending an email that purports to be from the company's CFO to the person authorized to send wire transfer instructions, but using the deceptive domain name. In this example, the "From" line of the email will appear as "From: Roger Black <RBlack@usa1001.com>." Notice the extra zero in this email address? Unless you were forewarned, you'd be very likely not to notice it. Instead, when Sandy Smith receives an email from RBlack@usa1001.com telling her to immediately send a wire transfer to a particular bank account (accompanied by a plausible explanation for why the funds should be transferred, often with legitimate-looking invoices attached), she may well do it.

A variation on this pattern is the use of a domain name deceptively similar to one of the target company's regular suppliers. In this kind of case, the fraudsters need to know the identity of who is selling to the target company, something that may require some inside information. Instead of impersonating a company officer with authority to order wire transfers, the fraudsters impersonate the company's supplier. Although the information required to put this scheme in play is harder to come by, once it is obtained, the fraudsters have a better chance of success, since the funds only need to be redirected to a bank account under the fraudsters control, but all other information fits the target company's usual course of paying invoices submitted by a known supplier. Information about a supplier can be gained by searching websites of companies likely to be selling to the target company, which may list the supplier's large customers, or through social engineering, e.g. by getting to know someone in the supplier's sales force and waiting for the identity of the supplier's large customers to be disclosed.

Where The Money Goes, And How To Get It Back (If You Act Fast)

The People's Republic of China (PRC) is often in the news as the origin of sophisticated hacking attacks on Western private and government computer systems. But it is also one of the main launching pads for the simpler kind of fraud. Fraudsters in the PRC often use bank accounts in Hong Kong as the first destination for the money they trick target companies into wiring.

Three Reasons Why Hong Kong Is The Favored Destination For These Wire Transfers

1. It is geographically close to the place from which the fraudsters work and it's relatively easy for them to travel to Hong Kong in person to set up the first-destination bank accounts.
2. It has a very active business and commercial environment in which banks are accustomed to seeing high levels of activity between PRC suppliers and Western buyers. New companies opening new accounts into which large amounts of money are wire transferred by Western companies is a common occurrence for Hong Kong banks. Fraudsters can take advantage of the pattern of normal, legitimate business to mask their activities; in essence, they can hide in plain sight by blending in with the crowd.
3. It has a vibrant entrepreneurial culture, so the legal mechanisms for creating new business entities are relatively easy for fraudsters to use to quickly set up a shell company cheaply for the purpose of creating a bank account.

Catching The Crooks

The people conducting these frauds know that they will be discovered quickly so their goal is to move the money they've stolen out of the original bank account as quickly as possible. However, in order not to trigger the banks' automated fraud detection systems, they have learned that moving the money instantly is not a good idea. They also know to not move the money out of Hong Kong (their ultimate goal) in a single step. Instead, they may leave some or all of the funds in the original bank account for a day or more, and then move it in increments to other accounts in Hong Kong they control. Those secondary accounts will have an established pattern of moving money offshore to destinations (often to places such as Vanuatu, Vietnam) where banking controls are scant.

This last point, coupled with Hong Kong's excellent legal system (still modelled after the English system under Hong Kong's "one country, two systems" political status) provides some hope to companies that have fallen prey to the fraud, but only if they detect the fraud and act quickly.

In responding to such a fraud and being armed with the details (copies of the emails implementing the fraud and details about the fraudster's account receiving the funds), the first step is to immediately contact the destination bank by telephone. Although banks usually won't confirm in a telephone conversation that the transfer has been made or that funds are in the account, they will usually freeze activity in the account for the few hours it takes us to initiate legal action. Simultaneously with making the first phone call to the destination bank's internal security department, a judicial process is started, in which the Hong Kong court will be asked to issue an order freezing the bank account and any other known assets of the person who has received the victim's funds up to the value of the total losses suffered by the victim.

Once the court has issued the freezing order, it will be served on the bank, enabling it to continue to freeze the bank account. A civil action will be initiated in which the victim will claim the funds it has been cheated out of, plus interest and legal fees and other direct costs of the litigation. The recipient of the funds will often not answer the civil action, enabling the victim to enter judgment on its full claim by default. Armed with a default judgment, the judgment can be enforced by attaching the funds frozen in the recipient's bank account, ultimately returning them to the victim. When making a freezing order the court will require the bank concerned to disclose full details of the recipient's bank account, including full details of any transfers out of the account so that the victim can trace its funds and see where they have gone. The underlying civil claim can then be widened to include the persons who received the victim's funds if they were sent on.

Protecting Your Business Against The "Email Imposter" Fraud

The most effective way to protect your business is to require a two-method verification: any email initiating a wire transfer to a new bank account should be confirmed with a phone call to the person purporting to order the payment. In the first example, this is a simple matter of a domestic telephone call from your accounting department to the CFO or comptroller who may be impersonated. In the second example, an overseas call to a known person actually employed by your company's Chinese supplier at a previously agreed telephone number is required. The small additional expense is warranted as a safeguard against fraud schemes which usually aim to steal hundreds of thousands of dollars.

Beyond this, alerting all personnel involved in the process of authorizing and initiating wire transfer payments to the nature of the fraud described is a strong protection against becoming a victim. Two things all people involved in your company's wire transfer procedures should be made aware of are 1) the risks arising from any communication from any source that directs payment to a bank account that has not been previously used to receive legitimate transfers, and 2) the possibility that email addresses may be used by fraudsters that are deceptively similar to your company's or your suppliers' email addresses.

Armed with these protections, your business is less likely to fall victim to the new version of a very old scam. If you do detect that money has been stolen in this way, act immediately.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact:

Greg Burch | +852 3465 0635 | gburch@lockelord.com
Adrian Taylor | +852 3465 0633 | ajtaylor@lockelord.com
Christie Yeung | +852 3465 0612 | cyeung@lockelord.com