What NOW

What should you do if you fall victim to a BEC scam?

MICHAEL S. KIM, RANDALL ARTHUR AND KELLY SPATOLA

Copyright ©2016 by the Association for Financial Professionals. All rights reserved in all countries.

KEY INSIGHTS:

- Time is of the essence. The faster you notify law enforcement and your bank, the better chance you have of recovering stolen funds.
- Go local. Don't forget to pursue fraudsters in the country where they and your stolen funds are located.
- You'll need a local lawyer to help you navigate local courts.

At our firm, we see an increasing amount of business email compromise. (BEC) scams. Treasury and finance professionals see this as well—but what can they do after their organization has fallen victim?

How do I know if my company has fallen victim?

Two of the most common types of frauds are CEO fraud and invoice fraud. The former is well known by now; variations include CFO fraud and treasurer fraud. The latter, invoice fraud, occurs when the IT system of a customer or supplier of your organization is hacked. The fraudsters will identify invoices due and payable by the company to the customer, then alter the payment details on the invoices and resend them to the company with a request to redirect payment to a new bank account, which is under the control of the fraudster.

It is not uncommon for the fraudster to have been hacking into the relevant IT system for a number of months prior to committing the fraud in order to monitor e-mail traffic and thus be able to convincingly impersonate the executive or customer.

All this is well known, and many organizations are taking steps to prevent BEC scams. But what happens when it occurs?

Where do stolen funds usually end up, and can a victim possibly recover such funds?

Funds misappropriated through BEC scams can ultimately end up in any jurisdiction in the world (but almost never in the country in which the defrauded company is located). In our experience, misappropriated funds often end up in jurisdictions such as Hong Kong, China, Cyprus, various Eastern European countries and various African countries.

Misappropriated funds can be transferred in and out of bank accounts in an instant. Thus, the longer it takes to discover a fraud, the less chance a company has of recovering its stolen funds. BEC scams generally are uncovered soon after they are committed; large and unusual transactions are red flags which can be noticed by senior management not targeted by the fraudsters. Invoice fraud often takes much longer to be discovered—usually when an unpaid supplier or customer raises queries as to payment of its invoices, which could be weeks or even months after the fraud has been committed.

If your company has been defrauded, the key to recovering misappropriated funds is to take immediate action, both in your company's local jurisdiction, as well as the jurisdiction to which the funds have been remitted. Any delays can severely jeopardize the chances of recovery.

Copyright ©2016 by the Association for Financial Professionals. All rights reserved in all countries.

What should a company do after discovering that it has been defrauded?

Once a company discovers that it was the victim of fraudulent activity, it should take the following steps:

Immediately report the fraud to the bank from which funds were fraudulently transferred. Wire transfers are not always instantaneous. Rather, for a variety of reasons, the bank may delay processing a wire transfer—particularly a transfer of large sums of money. Such delays may give both the victim and the victim's bank the opportunity to cancel or unwind a fraudulent transfer, if they act quickly enough. In our experience, companies that quickly discover and report fraudulent activity to their banks are more likely to recover stolen funds.

Report the fraudulent conduct to law enforcement agencies in the jurisdiction to which the funds were transferred. If possible, defrauded companies should contact these agencies at the same time as they contact their bank, because local police, including police in Hong Kong and China, may be able to freeze the account receiving the stolen funds, thereby stopping the funds from being withdrawn or further transferred.

Inform your company's in-house counsel of the loss. In-house counsel will need to determine, among other things, whether the loss suffered is covered by the company's existing insurance policies. If the loss is covered, your company should promptly inform its insurance company of the loss to ensure timely compensation under its policies.

Finally, retain local counsel in the jurisdiction to which the funds were transferred. Local counsel will be able to advise on the best legal strategy to recover the stolen funds—for example, commencing a civil proceeding to obtain a freezing order or a disclosure order. Local lawyers can also facilitate communications with local law enforcement agencies, as discussed in more detail below, thus increasing the chances of funds being frozen before they are further dissipated.

> "Communicating with law enforcement agencies in a different time zone and in a different language can be challenging and inefficient."

What is the best way to report to and follow up with local authorities?

Communicating with law enforcement agencies in a different time zone and in a different language can be challenging and inefficient. Victims of fraud also often make the mistake of reporting crimes through an authority's online reporting system, which can cause delays in processing the report (and thus increase the risk of the funds leaving the account before steps can be taken to freeze the account). We have found that taking the following steps will maximize a company's chances of early and effective police intervention:

Contact law enforcement agencies through an agent that lives in the jurisdiction and speaks the native language—preferably local lawyers who are accustomed to dealing with the police and can quickly take steps to begin recovery of the stolen funds should they have been successfully frozen.

If possible, communicate with law enforcement officials face-to-face, as this will help in expediting their investigations.

Provide law enforcement officials with detailed information about the fraud and related wire transfers, including any and all evidence in support. For example, any email correspondence with the fraudsters and wire confirmations showing the name and bank accounts of the recipients.

How does a company obtain a freezing order from local courts?

It is often the case that the victim of the fraud cannot (or does not want to) rely on local enforcement to freeze the recipient's bank account. This may be due to the police

Copyright ©2016 by the Association for Financial Professionals. All rights reserved in all countries.

not having sufficient powers in the relevant jurisdiction to freeze the account, or the amount that has been stolen is of a sufficient value that the victim wants take additional action to try and secure the funds. In this case, the victim should apply to the local court for a freezing order. Freezing orders—known as a Mareva injunction in Hong Kong or a property preservation order in China—prohibits the recipient of stolen funds from disposing of its assets, including withdrawing the stolen funds from the account. The bank will also freeze the account upon being served with such an order, making it impossible for the account holder to access the funds in the account.

In most BEC and invoice fraud cases, the victim can apply for a freezing order on an urgent and *ex parte* basis—*i.e.*, the victim is not required to notify the account holder about the application unless and until a freezing order is issued by the court. Although this significantly speeds up the process, note that it can take up to a day or two to compile all of the evidence needed and prepare the application, during which time funds can be transferred or withdrawn. It is thus important to retain local counsel early to aid in these efforts, so as not to further delay the process.

Given their draconian nature, there are often potential obstacles and pitfalls to be to be aware of when preparing an application for a freezing order. While the standard for granting such an order is high in most jurisdictions, if the victim can produce concrete evidence of the fraud, most courts will be inclined to issue a freezing order, at least at the ex parte stage. Also, some courts require that the victim provide a sum of money to the court—i.e., a bond—to obtain a freezing injunction. Companies should discuss with counsel whether and under what circumstances a freezing order might be possible and what requirements will need to be met to make such an application.

How does a company obtain information about the whereabouts of the stolen funds?

It is not uncommon for fraudsters to quickly and repeatedly transfer stolen funds to different banks in an attempt to evade detection. The most efficient way of tracing the funds is through the recipient banks themselves. Often, however, banks and the police are unwilling or unable to provide information about bank accounts without a court order. Therefore, consideration should be given to applying to the local court for a "disclosure order." This is an order requiring the bank to provide information about the account holder and whether and where funds were subsequently transferred. This can either be done as part of the freezing order application or as a stand-alone application (if, say, for example, the victim has become aware that the funds are no longer in the account but still wants to trace the onward remittance of the funds).

It should be noted that courts will often give banks a generous amount of time to comply with disclosure orders, typically seven to 14 days. Such delays may hinder tracing efforts, as it is very likely that fraudsters will continue to move the funds through different banks meaning it can often be difficult to locate the ultimate destinations of the funds. Again, it is important for a victim to move quickly when making a disclosure application in order to give itself the best chance of successfully tracing and freezing stolen funds.

What should a company do after the funds are successfully frozen?

Once the stolen funds (or some portion thereof), are successfully frozen, a victim should commence civil proceedings against the recipient for the return of those funds. If the recipient does not appear or otherwise defend the proceedings and commits an act of default, then a judgment can be entered against the recipient. A victim can then seek to enforce the judgment by applying for a third-party payment order (also known as a garnishee order) against the banks where the funds are held. Such an order requires the bank to remit the funds in the account to the victim in satisfaction of the judgment.

Michael S. Kim is co-founder and Randall Arthur and Kelly Spatola are attorneys with Kobre & Kim.

Copyright ©2016 by the Association for Financial Professionals. All rights reserved in all countries.