Bloomberg BNA

White Collar Crime Report™

CYBERCRIME

The Latest CEO-CFO Cyber Scam: How To Avoid It, And What to Do If You Have Been Hit




BY T. MARKUS FUNK, SELENA LINDE, TODD HINNEN AND ALEX BAILEY

U.S. companies of all sizes have lost millions of dollars in recent months to a simple yet highly effective and increasingly common cyber scam, based on social engineering and playing on fear, the desire to be helpful, and other emotions. Named the ''business email compromise'' by federal investigators, the scam is prevalent among companies with foreign suppliers or frequent financial wire transfers.

T. Markus Funk is a partner at the law firm of Perkins Coie LLP. He is the founding co-chair of the firm's Supply Chain Compliance practice. He can be reached at mfunk@perkinscoie.com.

Selena Linde is a partner in Perkins Coie's Insurance Coverage practice. She can be reached at slinde@perkinscoie.com.

Todd Hinnen is a partner in Perkins Coie's Privacy & Security practice. He can be reached at thinnen@perkinscoie.com.

Alex Bailey is an associate in Perkins Coie's Litigation practice. He can be reached at abailey@perkinscoie.com.

In what follows we summarize how the scam works, how to protect your company from falling prey to it and actions to take if your company becomes a victim of the scam, including an in-depth look at insurance recovery for losses incurred by the fraudsters' scam.

How the Cyber Scam Works

The scam has been successfully executed with various levels of sophistication. Here are the basic elements:

■ **Spoof/bogus company executive's e-mail address**. The fraudster spoofs an e-mail address or, less frequently, creates a similarly worded one that appears to match the e-mail address used by an upper-level manager, typically the chief executive officer of chief financial officer.

■ **Spoof email from company executive**. Using that spoofed e-mail address, the fraudster sends an e-mail to the company's treasurer or another senior administrator in the finance department. The e-mail often directs the treasury employee to immediately wire funds to a bank account, which is often located in Hong Kong, in connection with an ''urgent'' and ''highly confidential'' project (e.g., purchase, joint venture, etc.). The purported need for discretion and secrecy is typically highlighted.

 ISSN 1559-3185

■ **Fraudster call**. In addition to sending an e-mail, the fraudster will also occasionally place a telephone call to the finance department employee, reaffirming what was already stated in the e-mail. Note that the fraudster's gamble in sending the e-mail and placing the call is that the employee on the other end will be reluctant to question the high-ranking executive.

■ **A lawyer joins the mix**. In order to further buttress the apparent ''credibility'' of the request, the sophisticated fraudster may introduce by phone or e-mail a co-conspirator into the mix. Most frequently, this is a supposed ''lawyer'' for the fictitious ''recipient'' company with whom the company executive is working or negotiating. The employee then receives such a phone call from a purported lawyer, who provides further instructions.

■ **''Please send money to [Hong Kong/Moscow/etc.] bank account.''** The scam artist then provides wiring instructions and often includes a generic explanation of how the treasury employee should expense or record the transfer.

■ **Funds head overseas**. Believing the request to be legitimate, the employee wires the requested funds—in some cases millions of dollars—to the scam artist's account.

In our experience, the scam artists are articulate, convincing and tenacious, not to mention, on the whole, ultimately successful in their execution.

Protection Against the Scam

This scam relies largely on employees' eagerness to please their superiors, particularly a CEO or CFO, and the employees' consequent hesitation to question or push back on requests ''from above.'' To avoid the scam, companies should foster a culture—and institute corresponding policies and procedures—that encourages employees to be cautious about unusual requests, even when they come from the highest levels. Companies, for example, should have policies requiring confirmation of any substantial and unusual transfer of funds and rigorous internal controls that operate even at the highest levels.

We recommend that companies protect themselves by taking the following actions:

1. Conduct Due Diligence of Non-Routine Requests.

Review your policies to ensure that they require appropriate due diligence before the execution of wire transfers. The appropriate policy will empower and, in fact, require the employees to question all people in management, no matter his or her position and rank. Employees should follow these steps:

■ Carefully question and check the requester's e-mail address. In some instances, the scam artist uses an e-mail address that is very similar but not identical to the true address of the person he is impersonating (e.g., jdoe@genericcompany.com versus jdoe@generriccompany.com).

■ Confirm the request *not* by replying to the initial e-mail but instead by initiating an independent e-mail chain sent to the purported requester's known, correct e-mail address. The preferred option is to speak directly with the purported requester.

■ Ask appropriately probing questions about the purpose of the request, how it should be recorded and other facts that might reveal a fraudster.

Raise Awareness. The company should inform all officers and employees, particularly those who control company funds, of the nature of this scam. Employees should be cautious about any request for a significant transfer of funds to an unusual account or for an unusual purpose or in an unusual amount, no matter the purported author of the request.

2. Institute Preventative Procedures.

The company should establish unique procedures for non-routine wire requests that will mark such requests as legitimate. This could be as simple as requiring officers or employees making non-routine requests for funds to (1) use specific, unique language in the request (in effect, provide a password); and/or (2) copy the request to an internal e-mail account created for that purpose (e.g., *fundsrequest@company.com). Requests that do not follow established internal procedures would be treated with extra caution.

Steps to Take If the Scam Hits Your Company

Act Quickly—Don't Delay, No Matter How Embarrassing the Situation. If your company falls victim to this type of scam, know that you are not the first! While ''falling for'' a scam may be embarrassing, it is not uncommon and has happened to even the most sophisticated companies. In short, do not allow embarrassment to cause you or your officers or employees to delay reporting the fraud or taking remedial measures.

Beware of the ''test'' withdrawal prior to complete withdrawal. To have any chance of recovering lost funds, it is critical that your company act quickly. In our experience, once the funds enter the scam artist's account, he does not always immediately withdraw all the money—presumably out of concern that this would raise an obvious red flag with the bank. Instead, like a credit card thief who ''tests'' the card with a small transaction at a gas station, the scam artist normally withdraws only a portion of the funds shortly after the transfer. In short, sometime the funds may sit in the receiving account for days, weeks or even months.

As a consequence, it is important to ask (or, more likely, obtain a court order in the receiving bank's jurisdiction compelling) the receiving bank to ''freeze'' the account pending the outcome of the police and internal investigations. To the extent you catch the fraud within 24 to 48 hours, you should immediately ask the sending bank to unwind the transaction.

Retain Counsel for Guidance and Damage Control. As discussed above, there are a number of interconnected steps a company must take immediately in order to minimize the unfortunate losses typically associated with a successful fraud. Experienced counsel can guide your company through the labyrinth of requirements.

Contact Authorities. Even the most ''obvious'' fraud does not result in immediate action by the receiving bank. In our experience, the bank receiving the trans-

   ISSN 1559-3185

ferred funds will not simply reverse the transaction upon receiving notification of the fraud, no matter how obvious the fraud appears to be. However, the receiving bank usually is willing to (officially or unofficially) freeze the account pending resolution of the complaint, particularly if it is asked to do so by the FBI or a local law enforcement agency.

Investigate the Fraud. Work with outside counsel to develop an immediate work plan focused on determining what happened. This will entail reviewing the particular transactions and associated communications and interviewing those involved in the matter. Beyond that, however, many companies engage forensic accounting firms to help identify appropriate remedial steps to avoid future victimization. They also hire cybersecurity specialists to track down and react to any potential intrusions into the company's systems and to help to determine the identity/location of the perpetrator(s) in some instances.

As part of this investigation, the company should immediately work with counsel to do the following:

■ *Summarize Events*. Write up a short—three to four paragraphs are sufficient—plain-language summary of the basic chronological ''story'' of the fraud. Review the summary to ensure that it does not unnecessarily invite liability or litigation or interfere with insurance coverage claims.

■ *Inform the FBI and U.S. Secret Service.* Report the crime to the FBI and Secret Service. Do ask for assistance in freezing the account, but be realistic and know that the bulk of the effort focused on recovering the stolen funds will typically be expended by the company, not the authorities. Insurers, board members, investors and other stakeholders will expect the company to immediately contact the authorities, so this should be a high-priority action.

■ *Inform local (foreign) law enforcement*. Report the crime to law enforcement officials in the jurisdiction of the receiving account and ask for assistance in freezing the account.

■ *Inform transferring and receiving banks*. Report the crime to both the transferring and receiving banks. And, if the fraud is detected immediately, demand that the transferring bank ''unwind'' the transfer. The banks will typically request a copy of any report filed with the police.

■ *Review all potentially relevant sources of insurance and provide prompt notice*. Fraud claims may trigger many different types of insurance coverage, so the company should immediately review its entire portfolio upon discovery of the fraud and promptly notify all potentially relevant insurance companies.

Insurance Coverage for Scam Damage

Companies that fall prey to these types of scams may be able to recover under insurance policies. We recommend that companies, in close coordination with coverage counsel, take the following steps:

Step 1: Assess Potential Coverage.

While crime and fidelity policies are the first obvious insurance policies to review, do not overlook the possibility of coverage in your company's cyber policies, property policies, crisis policies and/or bundled liability policies. All of these policies may contain wire transfer fraud coverage, computer fraud coverage and forgery coverage, all of which may be applicable. Further, if the money stolen was not your company's money, but instead a client's money, there may also be a case to be made for coverage under certain errors and omissions policies. Do not be discouraged when policy exclusions may initially appear to preclude coverage. The case law in this area is still in its infancy and many policies contain ambiguous language that should ultimately be construed in favor of coverage. If you are unsure of whether coverage exists, you should reach out to experienced coverage counsel.

Step 2: Notify Your Insurers.

Once you have reviewed your policies, provide prompt notice of claims and determine whether to provide notice of circumstances under other policies. Your notice letters must conform to the requirements of the language in the particular insurance policy. Further, depending on the nature of the known facts at the time of discovery, you should consider entering into nondisclosure agreements with your broker and insurance carriers that are specific to the fraud. Companies should not wait until investigations are complete to provide notice. Instead, inform your insurance companies that you are still investigating and determining the facts and update them as the investigations proceed.

Step 3: Watch Your Words.

What you say to whom and how you say it, even in the initial notice letter, may make the difference between a covered and an uncovered claim. Be careful in the initial stages when characterizing your claims or discussing coverage with your insurance companies, your brokers or any outside consultants.

There are a number of issues that can significantly affect the existence or amount of an insurance recovery. For example, determining which coverage a claims falls within under a single policy may not be obvious and may require a legal judgment call that should not be made until the policyholder understands how the decision affects the amount and scope of the insurance coverage it may collect.

This could involve layers of analysis, including the law on the definition of fraud in all potentially relevant jurisdictions, the relevant deductibles, limits and sublimits under the policies and how the investigation into the fraud is developing. Outside coverage counsel can work with risk managers and in-house legal counsel to ensure that a policyholder meets its reporting obligations without compromising potential coverage. Policyholders should avoid being bullied into making premature calls.

Step 4: Select an Insurance Spokesperson.

To maintain a single cohesive message with insurers and your broker, you should identify one point of contact in your company who will communicate with the insurance companies, broker and outside counsel throughout the life of the claim. This is usually the risk manager or in-house counsel. In addition to carefully watching what is said to your insurance companies, this individual should also be careful when discussing coverage issues with brokers or any outside consultants. In

many jurisdictions, communications with a broker or outside consultants are not subject to any privilege. Thus, any unprotected communications may be discoverable if a coverage dispute ultimately arises.

Step 5: Carefully Manage Forensic Consultant's Scope of Work.

As touched on above, coordinating with counsel to conduct a rapid-response internal review of the who, what, where and when of the fraud is critical. And in order to properly conduct such a review, you will likely want to engage a forensic consultant.

The forensic consultant's scope of work should be limited to determining how the fraud occurred, tracing the money and, if applicable, how your company's computer system was breached. If the fraud is a covered claim, these forensic costs are usually covered expenses under your insurance policy.

Be aware, however, that if you expand the scope of work into a full analysis of your company's policies, procedures and security controls, the forensic reports may become discoverable in any future coverage litigation. Put another way, an expansion in the scope of work beyond the specific details of the current fraud could lead to ultimate findings by your forensic consultants that the insurance carriers may use to attempt to deny your claim or rescind your coverage. And when you feel it necessary to conduct such analysis in order to avoid future scams and to tighten your control, which may be in many such cases, be sure that you cloak this work with attorney-client and work-product privilege to the greatest extent possible.

Step 6: Demand Your Insurers Fulfill Their Coverage Obligations.

Policyholders must demand that their insurance companies meet all contractual obligations. They should not accept any denial as final. Instead, a denial is often the beginning of the dance with an insurance carrier.

If policyholders eventually need to file a lawsuit or to arbitrate against their insurer, they should review the policies and determine what steps need to be taken. Some policies contain mandatory waiting periods and mediation or arbitration prior to bringing a coverage lawsuit. Policies also may contain lawsuit limitation clauses that limit the policyholders' time to bring a lawsuit or notice arbitration.

Since this fraud scheme is fairly new and pervasive, policyholders should determine early which potentially relevant jurisdictions may apply and whether those jurisdictions have competing case law. If there is competing case law, the insurance company may ''jump'' the policyholder and file a declaratory judgment action in the less favorable jurisdiction. If you determine that you may have competing case law, you should consider filing a declaratory judgment action against your insurance carrier to preserve the forum of your choice.

Scam Prevention and Recovery Are Possible

Despite its simplicity, this type of scam has proven very effective. The amount of money lost in each case has typically been substantial—at least in the hundreds of thousands of dollars and as much as multimillions. Companies can avoid falling victim to this scam by promoting awareness and implementing relatively simple controls such as those discussed above. And, once victimized, a company should contact experienced counsel to help guide it through the various above-described steps aimed at recovering whatever may be left of the funds as well as protecting the company's reputational and other interests.

  WCR ISSN 1559-3185