2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

One Step Ahead — The Evolving Nature of Wire Transfer Fraud and Business Email Compromise

Increased Risks from Wire Fraud

There has been an ever-increasing rise in the number of wire fraud incidents involving both social engineering and email account hacking to lure parties to a transaction to wire money directly into a scammer's account. On July 12, 2018, the FBI issued a Public Service Announcement. According to the aforementioned report, between December 2016 and May 2018, there was a 136% increase in identified global exposed losses. The scam has been reported in all 50 states and in 150 countries. Furthermore, statistics compiled between October 2013 and May 2018 showed a total 41,058 U.S. victims, and $2,935,161,457.00 in total dollars lost in the U.S. alone.

Business Email Compromise (BEC) Attacks

When a business compromise email or wire fraud occurs it is not always the fault of just one person. As such, all parties involved in a wire transaction must be vigilant. As a result of the rise in wire fraud, discussions are being held across all industries from law firms to real estate firms regarding steps to prevent this epidemic from occurring.

The most common way that wire fraud occurs is by way of a "spoofed" email. Under this scenario, an individual may receive an email from his real estate attorney, whom he has known for years, regarding a change in wire instructions. The email may even be conversational, asking about the client's recent vacation. The email then advises that, in order to close on time, funds must be transferred to a different bank account, and instructions for doing so are attached. The client recognizes the attorney's name and email address, and without any verification wires money to the alternate bank account. However, in the rush to immediately to take action to ensure that the funds are wired prior to the closing, the client does not realize the email he just responded to is actually from paulsrnithlaw@yahoo.com instead of paulsmithlaw@yahoo.com—the attorney's real email account. The parties subsequently appear for the closing, only to get the dreaded news that no person wants to hear: the money was never received. It should be further noted that in most cases, unless immediate action is taken within 72 hours, the funds usually have left the country making the funds impossible to recover.

Wire Fraud in the Digital Age

In today's digital age of Facebook and LinkedIn, wire fraud schemes that rely on targeted email phishing have become increasingly common and sophisticated. By finding individuals who have not

enabled privacy features on their social media accounts and then using that publicly available data to craft believable, fraudulent emails, criminals trick businesses into quickly sending funds by creating fake, urgent situations. Frequently, victims do not even realize they have been duped until they confirm the transfer of funds only to learn that the money is already long gone.

Best Practice Tips

In light of the rise in wire fraud, the following are best practices for to implement in order to avoid becoming a victim. First, a law firm should be conducting security awareness training to make employees and their custom alike aware and suspicious. When receiving an email, one should always start with the assumption that they may be a potential target for an attack. As such, if an email seems suspicious, one should trust their gut instinct. Because many of the cyber criminals are overseas, the emails will often contain spelling and/or grammatical mistakes, which should raise a red flag. However, this is not always the case as the level of sophistication involving spoof emails is improving.

As noted in the example above, at a quick glance, would you be able to see the difference between these two email addresses: InsCO@gmail.com and the spoof, InsC0@gmail.com? Once a malicious actor has gained access to one party's email account and discovers an opportunity, *i.e.*, an ongoing real estate transaction, they will often wait for the most opportune time to send an email with fraudulent account details requesting a change in wire instructions. In other instances, threat actors simply create an email address and impersonate a known lawyer, real estate or title agent. Additionally, criminals may target and impersonate the CEO or CFO of a company and request that a large sum of money be wired to a fraudulent account. These emails will often portray a sense of urgency in an attempt to have targets immediately wire money before they have an opportunity to fully review the email's content and question its legitimacy. Therefore, it is imperative that individuals carefully review these types of requests and identify email inconsistencies. A last minute email request for money to be wired to a different bank account in another state, especially when key personnel are out of the office, should be treated as highly suspect. Other tips for being aware and suspicious include: do not trust any content received from unverified emails, especially with respect to financial information; never click links or open attachments from unverified emails, as they may install malware on your system that can make you more vulnerable to email account hacking; do not respond to emails or phone calls asking you to verify personal or banking information; and when verifying suspicious emails, do not rely on the phone number contained in the email signature, as it may not only be fake, but will perpetrate the fraud even further.

Second, law firms that regularly work on transactions that involve wire transfers must establish a written policy and procedure for same. Once that policy and procedure is created, an organization must then make sure that all staff who may be involved in a wire transfer are properly trained on the process. The policy and procedures should include, but not be limited to, the following steps. At the beginning of the transaction at issue, collecting and verifying the contact information from all parties involved, and prohibiting the use of any other non-verified contact information. It should further be explained to the all parties to the transaction, both orally and in writing, that all wiring instructions should be confirmed from this verified information before any wire transfer is made. Moreover, every e-mail signature, as well as any retention letter, should include a warning regarding the possibility of wire fraud and detailing the company's wire transfer policy. If email security is in question, wire transfer instructions, including bank account information, should be done in person whenever possible. If this cannot be accomplished, wire instructions should be sent via encrypted email or a secure client portal. If receiving a change in wire instructions via email, an organization should inform all parties that any

electronic wire instructions should not be followed unless confirmed via a phone call to the previously verified person and documented. Furthermore, all wire transfer instructions should be confirmed via telephone call to the previously verified designated contact person, and any instructions should be documented via follow-up email to that person's verified email or other correspondence.

Finally, because most experts agree it is not a matter of if, but when, that a data breach will occur, basic cybersecurity practices should also be implemented to ensure that a company's internal system is safe. This includes conducting regularly cybersecurity awareness training, including how to spot wire transfer scams, for all staff (including temporary), and on the proper use of social media accounts since hackers monitor and use information on these sites. All employees should also avoid the use of free web-based email, instead establishing their own secure company e-mail account via website domain. Consideration should also be given to using the services of a third-party provider who monitors domains to see if anyone is seeking to create a fraudulent email account using the organization's name.

Additionally, unique complex passwords should be used on all accounts and devices (at least 12 characters: letters, numbers and symbols). This also includes changing these passwords on a regular basis, and not using the same email and password combinations across multiple websites. As noted already, email involving sensitive personal identifiable information should be sent via encrypted email, and multifactor authentication should be used on all email and financial accounts. Lastly, an organization should protect its network perimeter with a firewall, and operating systems and software must be regularly updated to avoid malware attacks.