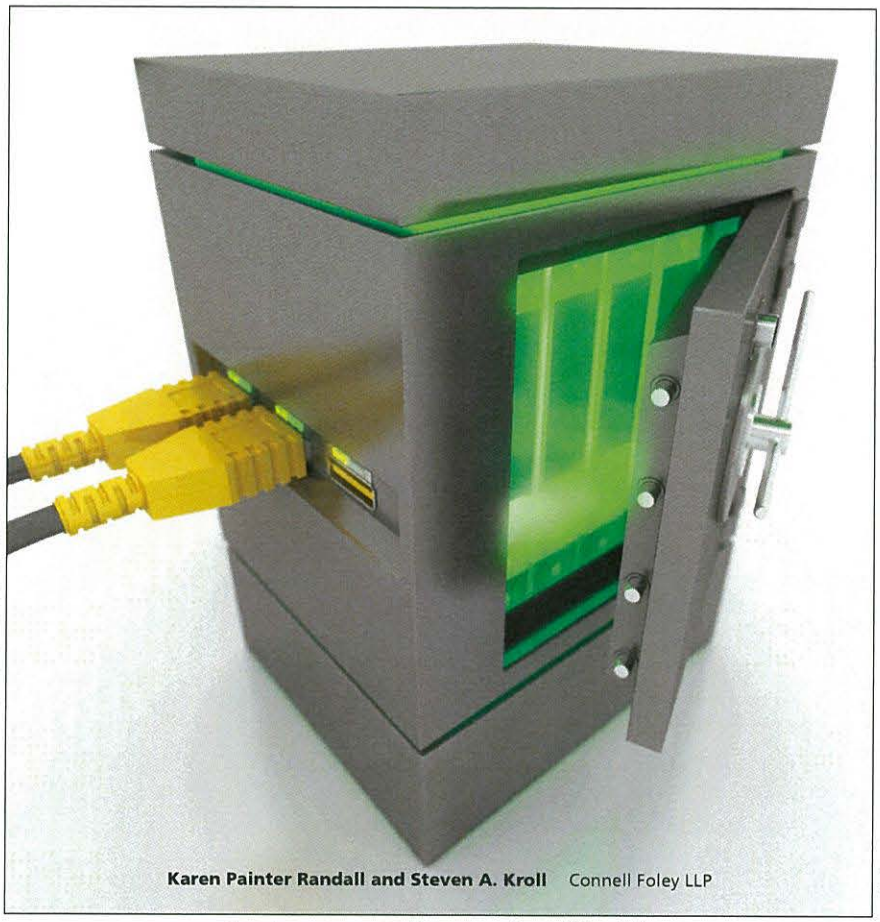
HERE TODAY GONE TOMORROW:

WIRE TRANSFER FRAUD



Karen Painter Randall and Steven A. Kroll Connell Foley LLP

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. In 2016, the FBI reported over $346 million had been stolen in these types of attacks. According to an FBI Public Service Announcement issued on May 4, 2017, between January 2016 and December 2016, there was a 2,370% increase in identified losses. Moreover, it was noted that Asian banks located in China and Hong Kong remain the primary endpoint of fraudulent funds; however, financial institutions in the United Kingdom have been identified as prominent destinations as well. Further, statistics compiled between October 2013 and December 2016 showed 40,203 domestic and worldwide incidents and that number is exponentially increasing.

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. In fact, in a Virginia "failure to warn" case, a plaintiff's attorney was held responsible for the damage caused by a spoof email for failing to also warn defense counsel who later wired settlement funds to an overseas account. 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. Thus, this article will focus on best practices to implement in guarding against becoming a victim of wire fraud.

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 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 j0hnsmithlaw@gmail.com instead of johnsmithlaw@gmail.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 and are impossible to recover.

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 avail-

able 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.

In light of the rise in wire fraud, the following are best practices to implement in order to avoid becoming a victim. First, an enterprise should be conducting security awareness training to make employees and customers alike aware of possible fraud scenarios. When receiving an email involving a change in wire instructions, the recipient should always start with the assumption that they may be a potential target for an attack. If an email seems suspicious, treat it as such. Because many cyber criminals are from overseas, the emails may 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 increasing.

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, InsCo@qmail.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, or 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, question its legitimacy and seek verification. 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 best practice tips 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, businesses 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 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 fax, 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, 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 cybersecurity awareness training, including how to spot wire transfer scams, for all staff (including temporary) twice a year, and on the proper use of social media accounts since hackers monitor and use information on these sites to perpetrate a scam. 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.

Because hackers are becoming more and more sophisticated in the way they seek to perpetrate these crimes, there is no silver bullet to prevent a cyberattack. As a result, an entity must remain vigilant to protect its customers' personal and confidential information. Nevertheless, by following the above steps, a company can greatly reduce its exposure and avoid being told that wired funds are not where they should be at the time of closing.

Karen Painter Randall is a Complex Litigation Partner with Connell Foley LLP in Roseland, N.J., and chair of the firm's Cybersecurity and Data Privacy and Professional Liability Practice Groups. She provides representation and advocacy services to professionals and businesses in a wide variety of complex litigation matters and is a veteran trial attorney in state and federal courts. Ms. Randall, vice chair of USLAW's Data Privacy & Security Practice Group and a former chair of USLAW's Professional Liability Group, is designated a Certified Civil Trial Attorney by the Supreme Court of New Jersey.

Steven A. Kroll is a Partner with Connell Foley LLP in Roseland, NJ. He is a member of the firm's Cybersecurity and Data Privacy Practice Group. In addition to representing professionals in various areas, Mr. Kroll concentrates his practice in the areas of professional liability and employment law matters in both New Jersey and New York. Mr. Kroll received his J.D. from Rutgers-Newark School of Law in 2009, cum laude, *and received the distinguished award of Order of the Coif.*