Avoiding Financial Fraud

BY AARON L. EVANS, KEITH D. LAPUYADE, AND JULIA HUITT

Mark, an attorney in Littleton, is staring at his computer in total disbelief. On Tuesday, he wired $750,000 to his client for proceeds from the resolution of a business settlement. On Thursday, his client called to tell him the money had not arrived in his account. Mark then verified the wire instructions with the client, which is when he realized that the wire instructions he used were fraudulent. The firm's bank could not reverse the transfer. Mark now faces the dauting task of notifying his malpractice carrier and hiring an attorney to act as his personal counsel in dealing with the insurance company (the malpractice carrier has coverage attorneys to represent its interests, which are not always the same as your interests; a personal counsel attorney can advise you on how to protect your interests as you go through the claims process). If only Mark had been aware of the constant threat of wire fraud that affects nearly every law firm.

Sally, a client of a law firm, receives a bill for $35,000, purportedly from the law firm's accountant (on a Sunday), with an urgent request to wire the funds as soon as possible. Sally is a realtor and is aware of wire fraud, but because she's flustered and trying to do several things at once, she goes ahead and wires the money per the email instructions. Luckily, Sally is able to claw the funds back before they leave her account, but that is not usually possible. After hearing of the incident, the firm reviews its policies and concludes that its internal controls over how wire transfers happen would not have stopped Sally from initiating the wire. The firm updates its retention agreement and its billing emails, along with the bills themselves, to indicate that the firm will *never* send wire instructions via email or request that payment be made by wire transfer.

Tom, an attorney, granted bill-paying authority to his office manager, Emily. Emily regularly receives high-dollar-amount invoices and pays them via ACH. At one point, Emily pays a $95,000 bill via ACH, and not long after, the vendor contacts her and asks why the payment was delayed. Emily then realizes her email had been compromised, and the scammer had inserted ACH instructions into an email purportedly from this vendor. The malpractice carrier denies the claim, but the cyber policy provides partial coverage.

Jane, a bookkeeper for a law firm, receives an email from the firm's receptionist asking her to change the bank account for her direct deposit. Jane makes the change, and on the day after payday, the receptionist comes to Jane and informs her that she never received her paycheck. Jane lets her know that she changed the direct deposit per her email, and the receptionist tells her that she never requested that her direct deposit be changed. Jane is horrified to realize that she sent that direct deposit to a scammer.

The examples above illustrate the types of attacks that lawyers and law firms face every day in this increasingly digital age. Further complicating matters, these attacks are becoming harder to detect as scammers develop newer, more sophisticated ways to deceive us. To protect our (and our clients') bank accounts, we must remain vigilant and use every tool at our disposal to avoid being the victim of financial fraud. This article explains some of the most common scams circulating right now and provides best practices for guarding against them.

Common Scams

Most of us know not to click on links or attachments that originate from people we don't know, but there are now so many more ways for thieves to insert themselves into our financial picture. Below are some of the most common scams circulating right now.

Business Email Compromise

Business email compromise (BEC) is a type of attack in which scammers get unauthorized access to a business email account, often through phishing or social engineering attacks, and once inside, use the trusted email to get financial information. This is what happened to Jane and the receptionist in the payroll scam above. Importantly, BEC scammers can continue the fraud even after the victim changes their email password by creating electronic rules that continue to divert some of the victim's emails to the scammer. In some cases, a completely

new email account is required once an attack has occurred.

Prevention: Talk with your IT professional about email security protocols, train employees on how to recognize phishing attacks, and put multifactor authentication in place for email access. Consider relying paper like we used to do before email intervened. For example, if an employee requests a change to their direct deposit account, get a voided check from the employee with the information for the new account.

Gift Card Fraud

Scammers will spoof a supervisor's email saying that they are in a meeting but need the employee to go get gift cards from a store and send them pictures of the codes. They will indicate that it is critical that it be done right away. This type of scam is especially effective with newer employees, who won't be as aware of what a manager would or would not do.

Prevention: Teach employees to check (hover over) the sender's email address to see if it matches the purported sender's legitimate email address. In this type of fraud, the email accounts usually contain the supervisor's name, but the email address does not match the corporate email address. When onboarding new employees, warn them of this possibility and also let them know that the manager will never make requests like this. Employees should also be taught to be wary of any request that threatens a terrible outcome if the task isn't carried out right away. Urgency is a typical scammer tactic and a very strong sign that you're dealing with a scammer. The scammer wants you to do something before you stop and think.

Client Billing Fraud

The scammer will spoof an email from another employee asking for a list of clients, their contact details, and the amount owed. The scammer will then send falsified emails to clients with payment instructions that send the funds to the scammer's bank account. This is what happened to Sally, the realtor. In Sally's case, had she not been able to stop the transfer, Sally could have argued she wasn't responsible for remitting money to the firm since she already remitted payment to the scammer and the firm didn't have the appropriate safeguards in place.

Prevention: Awareness is key. Alert your billing person of this type of fraud so they won't fall prey to an email like this. Educating clients is also necessary. Many firms are adding language to their engagement agreements detailing how their billing process works and from whom they can expect requests for payment; this information is reiterated on bills and on websites. For clients, typing the law firm's web address directly into the browser (not following links) and using their online payment option is usually the safest bet.

Wire Transfer Fraud

Scammers will spoof an email with wire instructions that request that the money be sent to the scammer's bank account. This is by far the most expensive fraud perpetrated on law firms and other businesses. Once scammers gain access to your email through BEC, any email that says "wire transfer instructions" is a winning lottery ticket for them. They will send the changed wire instructions with your email address (or one that closely resembles your email), including signatures, and attempt to redirect those funds. This is the type of scam Mark fell victim to.

Prevention: Once you have a relationship with a client that may involve wire transfers, tell them upfront that you will never change wire instructions in the middle of the process, nor will you send an urgent email requesting them to wire money. Never rely exclusively on written wire instructions. Once you receive or send wire instructions, you must verbally verify them. You can't rely on the phone number in the email for verification, because a scammer can change the phone number in the email as well. Use a known number (for instance, the other party's phone number as listed on their website) and call them to verify the wire instructions.

Because scammers use automated software to scan for keywords, using email subject lines with "wire instructions" is like waving a red flag. Although we've all been taught to use accurately descriptive subject lines when emailing, this is one instance where something more vague, like "document request," would be the better choice. Another way to avoid emailing wire instructions is to use a service such as ShareFile; saving the wire transfer instructions to the file-sharing service means it has been encrypted during transit, so it's much less likely to be compromised.

Additionally, callers are now able to make calls that spoof phone numbers for people who use VoIP phone systems. This means even if the call appears to be from your client, unless you can verify something that only the client would know, it's possible you're talking to a scammer. If you have any doubt about the identity of the person on the other side, ask them questions only your client would know the answer to, such as the nature of the legal matter or who their insurer is (anything that would not have been on an email chain).

Best Practices

There are people sitting in office buildings around the world who do nothing other than try to figure out new ways to separate you (and your clients) from your money. There really is no surefire way to avoid fraud, because even as we put safeguards in place, the scammers continue to evolve their tactics. At a basic level, every computer should have updated virus protection software installed, and all operating systems should have the latest updates installed. Firms should have password change policies in place, either enforced through their IT provider or requested on a monthly or quarterly basis.

According to Loren Sheets of DiscoverySoft IT,[1] here are some basic things you can do to avoid having your email compromised:

There are people sitting in office buildings around the world who do nothing other than try to figure out new ways to separate you (and your clients) from your money. There really is no surefire way to avoid fraud, because even as we put safeguards in place, the scammers continue to evolve their tactics.

- Be suspicious! If it looks even a little bit off, it may very well be from a scammer.
- Verify the email address of anyone who sends you a suspicious-looking email or requests sensitive information. In Microsoft Outlook, you can hover your mouse over the sender's name to see more information about that sender (email, phone number, etc.). But note that scammers have gotten better at spoofing email addresses, so even one that appears to be from the correct person may still be a scam. If there is ever any doubt, it is best to email or call the sender directly, using their known contact information.
- If you get an email from an outside vendor (e.g., Microsoft, Adobe, Amazon, Gmail), never click on the link in the email to reset your password or to conduct business with that vendor. If you receive a legitimate-sounding request from a vendor, go directly to their website (and type it in yourself, ensuring that the web address is correct).
- Don't use public Wi-Fi (coffee shops, airports, etc.) while using your laptop; hackers can intercept the information going across public networks and steal your passwords, gaining access to your email and your online activities.
- Use multifactor authentication wherever possible. This adds an additional layer of security for any confidential sites.
- Even if you use an email client, such as Outlook, know how to log in to your web-based email to monitor for server-side rules that are redirecting your email to an unknown party.
- If your computer starts acting differently, you could have a virus. Contact your IT professional and ask them to scan your computer to see if there's an issue.
- If you have any doubt about the legitimacy of an email, send it to your IT professional and ask them to review.

For wire fraud specifically, awareness is the first step. At your next firm meeting, talk about the possibilities of wire fraud and specifically educate the people who have financial responsibility within your firm. Have a written policy in place that outlines the prevention steps above.

What About Malpractice Insurance?

An attorney's typical reaction after learning of this type of breach, and after recovering from the headache and nausea associated with the issue, is to find solace in the fact that there is malpractice coverage that should afford protection under these circumstances. After all, the attorney or the firm's employees were simply negligent, not guilty of any intentional or fraudulent misconduct. Think again.

Professional liability policies frequently limit or exclude coverage for these types of cyber liability claims under the definitions, conditions, and/or exclusions in the policy. Insurers frequently cite cyber exclusions, intentional acts, and criminal acts, even though the intentional and criminal acts were not those of the insureds.

In one case, the law firm immediately restored the lost funds and sought reimbursement from its insurance carrier. The carrier took the position that these were funds that the firm was legally obligated to pay and therefore did not fall within the definition of "damages" in the policy.

One example of an exclusion is:

> Any claim for conversion, misappropriation, wrongful disbursement, improper comingling or negligent supervision by any person or client of trust account funds or property, or funds or property of any other person, *held or controlled at any time by an Insured* in any capacity . . . .

Courts analyzing the same or similar language have concluded the language (1) is unambiguous, (2) excludes coverage for any claims arising from or in connection with the conversion or misappropriation of client funds or property by anyone, and (3) does not require misconduct by an insured.[2]

In *ALPS Property & Casualty Insurance Co. v. Murphy*, an attorney negotiated a settlement agreement for his client in a collection action involving a bank, with the client agreeing to pay the bank a confidential settlement amount. The attorney subsequently received an email from a criminal actor posing as the bank's counsel with wire instructions for the settlement payment.[3] The attorney provided the wire instructions to the client, who then wired the funds to the criminal actor's account; the bank never received the settlement payment, and the funds were lost. The firm sought coverage for the lost funds, and the insurance carrier denied coverage.

The attorney's insurance carrier argued that the exclusion applied to exclude coverage for the claim because it arose from or in connection with the conversion or misappropriation of funds held or controlled at any time by an insured in any capacity or under any authority.[4] The court noted that the exclusion "states that the control may be 'at any time' and in any capacity or under any authority" and determined that "Murphy had the power and authority to direct the settlement payment during the time when he received and forwarded the instructions, so he controlled his client's funds."[5] The court noted that "the language of the exclusion is quite broad, encompassing any claim either 'arising from' or 'in connection with' certain actions 'by any person,' not only the insured."[6]

Lawyers cannot assume that there is insurance coverage for actions and omissions that result in the loss of client funds as a result of cyber schemes. Be familiar with your policy, especially the exclusions. Many exclusions and limitations are added by endorsement, so be familiar with the endorsements to the policy too. Your insurance broker can tell you what the policy covers, but their comments are not binding; the policy is. If you do not have someone in-house who is experienced with reviewing and interpreting insurance policies, consider retaining an experienced practitioner once a year to audit your renewal policy to make sure you have adequate coverage and coverage for which you think you are paying.

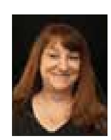
In addition, every lawyer and law firm should consider purchasing cyber coverage, which is a separate coverage, often with a different insurance carrier. The cyber policy should address issues relevant to a law practice, such as phishing, and specify that these types of claims are covered and not excluded under the cyber policy. Moreover, any discussion related to such coverage should be held with the insurance broker and/or in consultation with insurance coverage counsel, and should be confirmed in writing.

Conclusion

Awareness is the first step in protecting yourself and your law firm from financial fraud. Staying up to date on the latest scams and understanding how to avoid them is the second. While writing this article, we saw a new type of scam emerge where a stranger "accidentally" sends funds to a person through Venmo, and then asks the person to send the funds back. The person then sends the money back, only to discover that the original funds sent were through a stolen credit card. When the fraud is discovered, a chargeback is issued, removing the original funds from the Venmo account. The correct response is to let Venmo handle the return and not get involved.

As noted above, scammers are constantly evolving their attacks. The best defense is to make reviewing scams and computer intrusions part of your continuing education plan.





Aaron L. Evans is managing partner at Evans Case LLP, a probate litigation, personal counsel, and civil litigation firm in Denver. He has been practicing law for over 25 years with a focus on litigation in both elder and probate law, as well as handing all forms of estate administration—(303) 757-8300, evans@evanscase.com. **Keith D. Lapuyade** has more than 30 years of litigation experience in insurance law, bad faith, and fiduciary liability and has extensive experience with the representation of attorneys, physicians, and other professionals—(303) 757-8300, keith@evanscase.com. **Julia Huitt** is an accountant and CPA candidate with over 15 years of experience in billing and accounting for law firms in the Denver area. She owns LawyerCFO, a company focused on financial management for attorneys—(303) 209-9022, julia@lawyercfo.com.

Coordinating Editor: Chris Little, clittle7892@gmail.com

NOTES

1. Loren Sheets, lsheets@discoverysoftinc.com, is a CEO and senior network administrator at DiscoverySoft, which has been providing full-service information technology support in Colorado since 1999.
2. *ALPS Prop. & Cas. Ins. Co. v. Murphy*, 473 F.Supp.3d 585, 592–93 (N.D.W.Va. 2020) (exclusion was "broad" and excluded coverage for settlement payment lost to criminal actors after insured innocently provided fraudulent wire instructions to client's bank); *Attorney Liab. Prot. Soc'y, Inc. v. Whittington Law Assocs., PLLC*, 961 F.Supp.2d 367, 372 (D.N.H. 2013) (exclusion was "clear and unambiguous" and applied to "the misappropriation of, simply, 'funds' that are 'held or controlled by an Insured in any capacity or under any authority'"); *Fid. Nat'l Title Ins. Co. of N.Y. v. OHIC Ins. Co.*, 619 S.E. 2d 704, 708 (Ga.App. 2005). *See also Accounting Res., Inc. v. Hiscox, Inc.*, 2016 U.S. Dist. Lexis 135450 (D.Conn. Sept. 30, 2016) (accounting firm's professional liability policy excluded a claim that arose from theft of funds accomplished by criminal computer hackers regardless of who had done the theft or misappropriation).
3. *Murphy*, 473 F.Supp.3d 585.
4. *Id.* at 592.
5. *Id.* at 593.
6. *Id.* at 592.