Utah Lawyers and Licensed Paralegal Professionals:
Be on the lookout for this common wire fraud scam

Scams aimed at defrauding law firms have gained startling momentum in recent months. Just in August 2021, the Utah Bar received multiple complaints of internet fraud aimed at lawyers. This appears to track what the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center is also seeing in the general public. On May 15, 2021, the FBI revealed a "record increase in reporting," with 1 million cyber-enabled crimes being reported from March 21, 2020 to May 15, 2021.[1]

Cybersecurity is a critical component of any law practice as scammers have found increasingly clever ways of avoiding safeguards by posing as legitimate parties to a potential transaction. If you suspect you are the target of a wire fraud scam, you must act swiftly to avoid a catastrophic outcome, including inadvertent violations of the Rules of Professional Conduct.

Successfully avoiding wire fraud is possible, provided you're familiar with the pattern of such scams, you remain mindful of potential red flags, and you keep your ethical obligations front of mind.

Pattern of a wire fraud scam

While scammers are clever at devising false narratives to compel law practices to authorize illegitimate transactions, there are some notable trends.

These scams usually begin when a law practice receives a solicitation email or phone call from a potential client. The prospective client may have an email address that appears to be legitimate—containing a domain that is similar to an actual business—or the email address is real because a scammer has compromised the identity of a real individual or company. If a real individual's or company's email address has been compromised, the scammer may be privy to proprietary information that, when communicating with the prospective lawyer, makes the scammer seem even more convincing.

The prospective client often claims to be interested in a commercial, real estate transaction, or debt collection matter and moves quickly to memorialize a retainer agreement with the lawyer. Once the agreement is finalized, the "client" sends a check to the lawyer with instructions to deposit the funds necessary to finalize the transaction. Very quickly, the "client" will then ask the lawyer to wire the funds back to them, minus the lawyer's earned fee. The problem is this: the check is fraudulent, and the lawyer is now on the hook for funds wired from their own account.

Scammers posing as clients always communicate with a sense of urgency, noting that the transaction must be "completed in the next 48 hours" or "this is a once in a lifetime opportunity!" This urgency is, of course, a vital strategy in committing the fraud before it is detected.

Red flags

- You are being contacted by an unknown individual who is requesting your services for a high-priced transaction.

[1] "IC3 Logs 6 Million Complaints," FBI.gov, https://www.fbi.gov/news/stories/ic3-logs-6-million-complaints-051721, last accessed August 24, 2021.

- You are being contacted exclusively via email or social media.
- A prospective client appears rushed to initiate the agreement and uses language indicating that time is of the essence.
- There are variations in the spelling of the domain name in the email address, such as mary@adobee.com. This appears to have come from Mary at Adobe, but an additional e has been added to the domain.
- You receive requests for guidance on transactions outside of your practice area. For example, you are a family law firm but are receiving an inquiry about negotiating a commercial real estate transaction.
- The recipient of the funds is in a foreign country.

What you can do

- Ask to meet in person or over a Zoom video call. This might scare the scammer away because they will suspect that you are onto them.
- Ask your bank for guidance on the check. National banking regulations require employees and agents to be up to date on appropriate screening and fraud procedures.
- If the funds have already been wired, immediately notify all impacted parties (if the scammer is posing as a real company for example), including the financial institution.
- Contact state authorities and file a complaint with the FBI's Internet Crime Complaint Center.
- Report the incident to your malpractice insurance carrier.
- Craft a cybersecurity policy for your firm that includes email security measures, authentication, and staff training, and stay up to date on new variations of business scams so you that you can spot them quickly.
- Be skeptical!

Ethical considerations

Unfortunately, a lawyer who has fallen victim to a wire fraud scam may face a disciplinary investigation if the release of the wired funds causes their IOLTA account to be overdrawn. There is also no assurance that such episodes will be covered by malpractice insurance.

Make sure you are up to date on relevant safeguards

The Rules of Professional Conduct apply to lawyers and, where consistent with a licensed paralegal practitioner's permitted scope of practice, to licensed paralegal practitioners. The term "lawyer" may encompass both practitioners.

Rule 1.1 (competence), comment 8 states, "to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*…" This recent amendment to the Rule incorporates language indicating that technological compliance is a necessary component of a lawyer's overall competency.

Make sure supervised lawyers and nonlawyer staff are adequately trained on cybersecurity best practices

Rule 5.1 (responsibilities of partners, managers, and supervisory lawyers) requires firms to implement strategies to ensure all firm lawyers are abiding by the Rules of Professional Conduct. Comment [2] states, "such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced legal professionals are properly supervised." Rule 5.3 imposes the same standard for nonlawyer assistance. Together these Rules impose an obligation to ensure that all employees within a practice (lawyer and nonlawyer) are adequately trained to abide by the Rules of Professional Conduct (including competency and confidentiality concerning client data, noted previously.)

If you are positive that a fraud has occurred, report the incident to the proper authorities

Rule 1.6 of the Rules of Professional Conduct affirms the necessity of keeping client confidences. The rule states in relevant part, however, that "a lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary…to prevent the client from committing a crime or fraud that is *reasonably certain* to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services." R. Prof'l C. Rule 1.6(b)(2).

Immediately distance yourself

You also can swiftly withdraw from the matter pursuant to Rule 1.16 if a fraud is underway. Under Rule 1.16(b)(3), a lawyer may withdraw from a representation if "the client has used the lawyer's services to perpetuate a crime or a fraud." The rule also allows for withdrawal if "other good cause for the withdrawal exists."

Conclusion

Being aware of these patterns is critical to avoid falling into a scammer's trap. Remember: If it seems too good to be true, it probably is!