Affinity Programs

PROFESSIONAL COUNSEL℠

Advice and Insight into the Practice of Law®

Wire Transfer Fraud: A Growing Threat to Law Firms

The practice of law involves advising clients on the risks and benefits of potential courses of action. Examples range from helping a client decide whether to accept or reject a settlement offer to analyzing whether a proposed contract provision will help or hinder a client's business objectives.

Lawyers, of course, must often serve as their own risk managers in managing their professional practices. Two of the primary risks involve maintaining the confidentiality of information relating to client representation[1] and safekeeping the property of clients and third parties.[2] These vulnerabilities have intensified due to the pervasive threat of cyber criminals who perceive law firms as repositories of valuable information and significant funds on behalf of clients and others. These bad actors can undo months or even years of a lawyer's hard work with a few well-placed keystrokes and a law firm lacking the tools and resources to address this exposure.

These bad actors can undo months or even years of a lawyer's hard work with a few well-placed keystrokes and a law firm lacking the tools and resources to address this exposure.

Wire Transfer Fraud Attempts Are Increasing

Lawyers in any area of practice may fall victim to wire transfer fraud, but the problem is most acute in real estate practice – both residential and commercial. Professional services pertaining to real estate matters present an inviting target for cyber criminals, since the parties and lawyers involved in such transactions often exchange sensitive financial data, face time pressure related to closure, and wire large amounts of funds. The FBI's Internet Crime Complaint Center's ("IC3") data confirms the growing trend in wire transfer fraud. From 2017 through 2019, the IC3 reported the following cybercrime data involving real estate/rental complaints:

Year	Number of Complaints	Reported Losses
2017	9,645	$56.2 million[3]
2018	11,300	$150 million[4]
2019	11,677	$221 million[5]

While not every complaint and reported loss in the above data involved law firms or their clients, the FBI reports reflect a number of cases involving the legal profession. In addition, CNA claim data for the same time frame demonstrates an increase in total incurred losses for law firms defrauded by wire transfer schemes.

1 *ABA Model Rule of Professional Conduct* 1.6
2 *ABA Model Rule of Professional Conduct* 1.15

3 FBI, Internet Crime Complaint Center, *2017 Internet Crime Report* 3, available at https://pdf.ic3.gov/2017_IC3Report.pdf (2017 IC3 Report).
4 FBI, Internet Crime Complaint Center, *2018 Internet Crime Report* 3, available at https://pdf.ic3.gov/2018_IC3Report.pdf (2018 IC3 Report).
5 FBI, Internet Crime Complaint Center, *2019 Internet Crime Report* 3, available at https://pdf.ic3.gov/2019_IC3Report.pdf (2019 IC3 Report).

Claim Scenarios

Although the following scenarios are fictional, they are based upon actual examples of wire transfer fraud schemes involving law firms.

Scenario 1

Jane works as a residential real estate lawyer with a high volume of clients. She relies on her paralegal to organize the closing documents and coordinate the details of the closings with clients and other parties to the transaction. In one closing, where Jane represented the buyers, Jane's paralegal received an email that purportedly came from the attorney for the sellers. The email address from which the email originated differed by only one letter from the correct email address of the sellers' attorney, but Jane's paralegal did not notice this discrepancy. The paralegal encountered an example of email spoofing – a form of social engineering employed by cyber criminals to trick the email recipient into believing that the email was sent from a trusted source.

The email stated that the sellers wanted the funds for the transaction to be wired to a different bank than the sellers' attorney had initially provided. In the email, the sellers' attorney explained that he had made a mistake in his prior email and that the initial bank he had listed related to a different transaction and apologized for any confusion. Jane's paralegal followed the new instructions in the most recent email, without informing Jane or calling the sellers' attorney to confirm that the new wiring instructions were valid. Of course, cyber criminals had sent the new wiring instructions and stole the funds intended for the real estate sale.

With more lawyers and support staff working remotely, law firms must ensure that their network is accessible to authorized users, while also secure from outsiders and bad actors.

Scenario 2

Jim represents plaintiffs in personal injury matters. In a recent case, Jim negotiated a favorable settlement for his client. During the negotiations, Jim received an email containing poor grammar and spelling that his client purportedly sent. The email also included different wiring instructions for the settlement funds than the client had previously provided to Jim. Jim sensed that he had received a phishing email – another form of social engineering, in which scammers send an email and impersonate a person or entity considered trustworthy by the target and seek to obtain sensitive information or data that can be used for financial gain. Jim immediately called his client, who confirmed Jim's suspicions about the fraudulent nature of the email. Jim deleted the email without responding to it but did not warn defense counsel of the attempted cybercrime.

Several days after he received the phishing email, Jim contacted the defense and inquired as to the delay in receiving the settlement funds. The defense attorney, confused by Jim's inquiry, explained that he had wired the funds three days ago, per Jim's email that contained the new wiring instructions. Knowing that he had never sent such an email, Jim realized that cybercriminals had deceived his opposing counsel, meaning that the funds intended for Jim's client were now missing and not likely to be recovered.

Scenario 3

Viola serves as the department head of the merger and acquisitions department of an international law firm. While representing her clients in the purchase of a large business, hackers breached email communications between her client and the parent company of the business that was being sold. In the phishing emails sent to Viola's law firm, the hackers claimed that the original account where the money was to be wired was under audit and gave wiring instructions for a different account to an overseas bank. Sensing potential trouble, Viola made a telephone call to the law firm for the parent company and left a voicemail message, which was not returned. The hackers forged additional documents and authorization letters concerning the new account at the overseas bank, which Viola assumed were being sent to her in response to her voicemail message. Upon receipt and review of these new documents, she authorized release of the funds, which went straight to the hackers' overseas account.

Risk Control Tips

Several important risk control lessons may be learned from the claim scenarios described above.

Train your support staff

As Scenario 1 demonstrates, continuous employee training should be implemented, focusing on social engineering schemes, which can result in wire transfer fraud or other cybercrimes. Supervisory lawyers are responsible for making reasonable efforts to ensure that the conduct of a support staff member is compatible with the professional obligations of the lawyer.[6] Such training should help law firm staff members identify email spoofing and other targeted phishing emails and also provide clear instructions on what to do when in receipt of suspicious emails. In order to be more confident that email senders are who they purport to be, type the name of email recipients instead of hitting "reply." Training also should instruct law firm staff to avoid clicking on unfamiliar links and attachments from unknown senders. Law firms may wish to consider testing their employees by sending them simulated phishing emails to determine whether or not they are applying their training on data security to their routine activities and the scenarios they encounter.

Share information on cybercrime attempts with all relevant parties

In Scenario 2, the lawyer thought that merely identifying and deleting a phishing email fulfilled his duty to his client. The existence of the phishing email, however, should have placed the lawyer on notice that cyber criminals obtained confidential information about the settlement agreement and might attempt to steal the settlement funds by deceiving other parties involved in the settlement. The lawyer, therefore, should have warned opposing counsel to be alert for a phishing email such as the one that he had received. Courts have held that where one party fails to exercise ordinary care that substantially contributes to a loss, such a loss must be borne by that party.[7]

Mandate dual authentication for wire transfers

Before wiring client funds, lawyers always should initiate a phone call to the intended recipient (or the intended recipient's lawyer) to verify the wiring instructions. Lawyers should call phone numbers known to be valid, rather than phone numbers referenced in e-mails that purport to confirm the wiring instructions. If any sudden and emergency changes to prior wire instructions occur, law firms should be on high alert and verify that the changes are authentic. Moreover, a written response to a telephone message is insufficient, as delineated in Scenario 3. Oral confirmation of wiring instructions must be provided, preferably by an individual whose voice is known to the lawyer or support staff member making the call. To convey their commitment to dual authentication, law firms also may wish to consider inclusion of disclaimer language to their outgoing email messages and website that the law firm will not wire transfer funds absent such a protocol.

Use caution when wireless/remote

With more lawyers and support staff working remotely, law firms must ensure that their network is accessible to authorized users, while also secure from outsiders and bad actors. Most law firms use virtual private networks (VPNs) to facilitate individual remote access. VPNs create a secure tunnel between a lawyer's local network on one end and the law firm's network on the other end across a public network (i.e., the internet). Data traveling within the tunnel is encrypted and, if intercepted, is indecipherable.

Encrypt emails

All emails should be encrypted, whether in transit or at rest (a/k/a end-to-end encryption). Encryption secures confidentiality by transforming emails sent and received by the law firm into an unreadable format for unauthorized users. Many successful wire transfer schemes occur when law firm personnel use non-secure email communication systems. Email encryption, however, is only as secure as the account from which it originates. For example, if cybercriminals obtain access to a lawyer's email account and password, through a phishing scam, they will be able to view the emails in the lawyer's inbox in an unencrypted (i.e., readable) format.

Consider client portals

Secure client portals offer an additional safety measure for law firms. Instead of accessing sensitive messages or documents via email, clients will receive an email notification that there is an item awaiting their review in the portal. Through the portal, the clients click on a link, enter their login information, and access the content contained in the message on a cloud-based platform. Sending wire transfer information via secure client portals reduces the risk of confidential information being breached.[8]

6 *ABA Model Rule of Professional Conduct* 5.3
7 *See Bile v. RREMC, LLC*, 3: 15-cv-051, 2016 WL 4487864 (E.D. Va. Aug 24, 2016).
8 See the CNA publication *For Your Eyes Only: Securing Lawyer-Client Communications* (April 2020)

Practice good Information Technology ("IT") hygiene

All law firm IT devices should be equipped with up-to-date antivirus and anti-malware solutions. An IT professional should ensure that all software updates and security patches are implemented on a timely basis. Sound password protocols help deter data breaches. Law firms should require strong passwords, preferably 8 to 20 characters, with a combination of capital and lowercase letters, numbers, and characters. Access to the law firm's network also should require users to change their passwords on a quarterly basis. In addition, the law firm should implement multi-factor authentication for account access, irrespective of whether the firm uses a VPN or a web-based provider via email access. If someone attempts to login from an unknown browser or IP address, a code will be sent to the user's designated cell phone number in order to gain access.

Vet your vendors

Law firms frequently outsource various tasks, such as file storage or eDiscovery services, to third-party vendors. Scammers will sometimes obtain confidential law firm data by hacking through the network security of a third-party vendor that is providing outsourcing services to the law firm. Lawyers have ethical duties to ensure that their vendor's conduct aligns with the professional obligations of lawyers, which includes the duty of confidentiality.[9] Law firms should inquire about the cyber security practices and other safety protocols of potential vendors in order to safeguard against the inadvertent or unauthorized disclosure of client or law firm information.

Discuss cyber and other insurance coverage with your insurance broker

Since wire transfer fraud and other social engineering crimes may involve the release of company funds by a person within your law firm – standard lawyers' professional liability policies may not cover your losses. Even a law firm with comprehensive preventive protocols may fall victim to social engineering fraud. Your lawyers professional liability policy should include coverage for social engineering, subject to the terms and conditions of the policy. If it does not include such coverage, your claim may not be covered. To help insure your law firm against wire transfer fraud and other scams, contact your insurance agent or broker to ensure that your law firm has the appropriate insurance coverage for this exposure.

9 *ABA Model Rules of Professional Conduct* 5.1 and 5.3.

Conclusion

Law firms face an increased threat of wire transfer fraud via social engineering schemes from cyber criminals. Preparing for this reality prior to an attempt may prevent or minimize the damage such fraudulent schemes can inflict upon law firms. Continuing education and vigilance surrounding this threat, including sound risk control and IT practices, provide the safest path for law firms and their clients in navigating the complex issues of today's cyber environment.

This article was authored for the benefit of CNA by:

Sean Ginty

Sean Ginty is the Risk Control Director for CNA's Lawyers Professional Liability Program. He collaborates with other CNA Risk Control lawyers on the design and content of lawyers' professional liability risk control services, products and publications. Sean lectures frequently at CNA-sponsored events and at state and local bar associations and national seminars hosted by industry-leading organizations. He also writes articles focusing on law firm risk control and professional responsibility issues. Prior to joining CNA, he served as Chief of Staff and General Counsel for an Illinois state agency and practiced law with a Chicago-based law firm, as well as serving as conflicts counsel for an international law firm. He is admitted to practice in Illinois and United States District Court, Northern District of Illinois.

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com