PROFESSIONAL COUNSEL®

Advice and Insight into the Practice of Law®

Top 10 Risk Control Tips to Avoid Wire Fraud Scams

Incurred losses for wire fraud have increased consistently on an annual basis for the past five years. So how can law firms protect themselves from falling victim to a wire fraud scheme? We strongly suggest that law firms evaluate the feasibility of implementing the following ten measures to protect themselves, their clients, and third parties from wire transfer fraud.

Mandate dual authentication for wire transfers.

Before wiring any funds, lawyers should initiate a phone call to the intended recipient (or the recipient's lawyer) in order to verify the wiring instructions. Lawyers should call phone numbers known to be valid, rather than phoning number referenced in emails that purport to confirm the wiring instructions and speak to a known party or party's representative. Some sophisticated schemes employ deepfake voice technology to mimic a person's voice. Law firms may be able to combat this threat by insisting upon a live discussion, rather than a voicemail message and staying alert for unusual word choices, tones of voice and inflections.

Slow down when wiring instructions are changed at the last minute.

Law firms should be vigilant to the potential for fraud in the event of any sudden or emergency changes to previously arranged written wire transfer instructions. Often, these requests indicate a need to receive the funds immediately and are made on a Friday afternoon or before a holiday. The purported recipient's alleged crisis should not distract the law firm from following the sound risk control protocols outlined in this article.

Examine URLs and email addresses carefully to ensure authenticity.

Cybercriminals often employ spoofing and phishing emails to law firms hoping to deceive lawyers and support staff to wire funds to entities and bank accounts that appear to be authentic but are, in fact, fraudulent and controlled by the fraudsters. These schemes can often be thwarted by closely checking for misspellings and slight deviations between the correct email addresses and account numbers and phony ones.

Educate your lawyers and support staff on wire transfer fraud schemes.

Law firms should hold regular educational programs for lawyers and support staff focused on social engineering schemes, which can result in wire transfer fraud and other cybercrimes. Teaching should include warnings to avoid clicking on unfamiliar links and attachments from unknown senders.

Test your employees' ability to identify cybercrimes.

Some law firms employ cybersecurity companies to launch simulated social engineering attacks on their employees in order to assess the law firm's readiness to repel actual cybercrimes. Please see CNA's Lawyers Allied Vendor Program for further information on contracting with such a cybersecurity company.

Use virtual private networks for remote access.

With more lawyers and support staff working remotely, more 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 the internet, encrypting all data flowing between the remote individual lawyer/support staff member and the law firm.

Utilize client portals for greater security.

Clients or law firms can implement secure web-facing portals to transact certain types of financial transactions and other business with greater protections than relying upon customary email. Using one of these portals, clients may click on a link, enter their login information, and access content from, or send, sensitive information to the law firm on a cloud-based platform, making it a more secure and effective channel to arrange for wire transfers. Please see CNA's Lawyers Allied Vendor Program for further information on contracting with such a cybersecurity company.

Encrypt sensitive emails.

If law firms do not want to use client portals, they should be encrypting emails that contain confidential sensitive data. Encryption secures confidentiality by transforming emails sent and received by the law firm into an unreadable format for unauthorized users. Please see CNA's Lawyers Allied Vendor Program for further information on contracting with such a cybersecurity company.

Keep software updated and establish a robust password policy.

Sound cyber hygiene protocols will add layers of protection to a law firm's network systems. Remain up-to-date with the most current software versions to patch security holes and require employees to use lengthy passwords (with upper and lower case letters, numbers and symbols) that must be changed on a regular basis.

Inform relevant parties of any cybercrime attempts when appropriate.

If a law firm successfully foils an attempted wire transfer fraud as described in these guidelines, it also may be required to notify opposing counsel of the attempt. For example, if a phishing email puts the law firm on notice that cybercriminals may have obtained confidential information about the wire transfer protocols, financial arrangements and institutions, or equivalent confidential or proprietary information of the law firm or the opponent, the law firm may have a duty to notify the other parties so that they can take reasonable steps to prevent being victimized by similar tactics. 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.[1]

1 *See Bile v. RREMC, LLC,* 3: 15-cv-051, 2016 WL 4487864 (E.D. Va. Aug. 24, 2016)

About CNA Professional Counsel

This publication offers advice and insights to help lawyers identify risk exposures associated with their practice. Written exclusively by the members of CNA's Lawyers Professional Liability Risk Control team, it offers details, tips and recommendations on important topics from client misconduct to wire transfer fraud.

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