Atty Insurance Implications Of Rising Nonclient Cyber Claims

By **Joseph Francoeur and Eve Soldatos-Mouzouris** (April 30, 2025)

Joseph Francoeur

Eve Soldatos-Mouzouris

Cybersecurity threats to law firms are on the rise.

It is estimated that 4 in 10 law firms experienced a security breach in 2023[1] and that in 2024, 42% of law firms with 100 or more employees had experienced a data breach.[2]

Law firms are considered prime targets for cybercriminals for several reasons, including:

- Law firms store highly sensitive client data.
- Many firms fear reputational damage and loss of critical case data, and feel forced to pay a ransom, fueling even more attacks.
- Many firms delay adopting top-tier security protocols.
- Busy lawyers often overlook red flags in phishing emails.
- Firms interact with external vendors, such as e-discovery services, which introduce additional security risks.[3]

Cyberattacks targeting law firms can take a variety of forms such as email phishing and malware attacks, distributed denial-of-service attacks, ransomware, and insider or third-party attacks.[4]

The effect of these law firm cyberattacks has been stark — a sharp increase in claims by clients as well as nonclients against lawyers.

This article addresses the reasons law firms are being targeted both for cyberattacks as well as claims by nonclient parties. Making matters worse, while claims by nonclients do not typically survive motions to dismiss, claims arising from cyberattacks are finding traction, thereby increasing the scope of exposure that attorneys face in their practice.

Verifying Wire Transactions

Both clients and nonclients can sue an attorney if that attorney was the party responsible for verifying wiring instructions. Lawyers have tried to evade claims for failing to verify wire

instructions, but to no avail. For example, in Palm Avenue Hialeah Trust v. Eisenberg, the U.S. District Court for the Southern District of Florida denied a law firm's motion to dismiss on March 13, finding that the law firm could not rely on the "apparent authority" of an individual to give them instructions to wire client funds to an unrelated third-party entity.[5]

In Palm, the law firm defendant argued that it did not breach the standard of care owed to its client when it wired funds belonging to its client to an unrelated third-party recipient over whom its client had no control or interest. The law firm had received instructions to wire the funds from an individual acting with apparent authority to oversee a litigation undertaken to enforce the client's rights as lienholder.

The law firm never verified the wiring instructions with the client, and the monies were sent to the unrelated third party. While the apparent authority was a creative argument in its defense, the court disagreed and found that there was no evidence that the client represented to the law firm that the individual had authority to direct wire payments.

Additionally, on the same day, the Superior Court of New Haven, Connecticut, recently found a law firm liable in Ferentini v. Mancini Provenzano & Futtner LLC, a case where an email compromise led to a client wiring approximately $90,000 to a fraudster.[6] The court found that the fraudster gained access to the law firm's email system and used it to request funds shortly after the plaintiff received a "clear to close" notice.

The court also noted that a similar incident had happened to another client in the past, and the law firm had failed to follow its own policies and procedures. In its defense, the law firm argued that the plaintiff had contributed to her loss by not following information in a cyber fraud warning contained in the law firm's introductory email, which stated that the law firm would never ask a client to wire money by email.

Despite this warning, the law firm had sent the plaintiff real wire instructions after, unbeknownst to the law firm, the plaintiff had already wired the funds to the fraudster. As such, the court found that the law firm had failed to follow its own policies, i.e., never ask a client to wire money by email and verify wire instructions.

Detecting Red Flags

In February, the Florida Bar issued a warning to lawyers regarding scam emails, which recounted the experience of an attorney who received an email that appeared to come from a local county government office, offering a legal consulting opportunity.[7]

The attorney stated that the email and interaction appeared real but that later "subtle red flags" were discovered, including an odd email address and grammatical mistakes. The scammer provided the attorney with a zip file, which the attorney downloaded. Luckily, the file was flagged by the attorney's security software as a Trojan virus, stopping it just in time.

Additionally, in November, U.S. federal courts issued a warning to all attorneys regarding fake electronic filing notifications purporting to come from the federal judiciary's Case Management/Electronic Case File system.[8] The public alert stated that the fake notifications prompt the recipient attorney to reply immediately and contain a link to access fake documents that "direct users to a malicious website."

Furthermore, in 2023, the New Jersey Supreme Court issued guidance on notifying the

judiciary if it becomes known that a user account may have been compromised.[9] The judiciary stated that it had implemented interlocking steps to protect against cybersecurity threats including multiple automated processes to scan and screen incoming communications and filings, in addition to requiring users to complete two-factor authentication.

Nonclient Lawsuits Upheld

Unfortunately, cybersecurity breaches turn into data breach lawsuits, which have been trending upward and show no signs of slowing. However, what is surprising is how these attacks can give rise to lawsuits and grievance complaints from nonclients against attorneys.

Typically, a nonclient cannot sue an attorney for professional negligence or malpractice because the attorney's legal duties are restricted to their client, i.e., lack of privity. The lack of privity defense is used to protect attorneys, but cyber threats are wreaking havoc on this protection.

This is especially true in wire transfer scams, where an email account is hacked by a cyber scammer who intercepts email communications involving a transfer of funds — for instance, a litigation settlement, a real estate purchase or a corporate transaction — and provides fraudulent wiring instructions. However, claims for contribution made by the nonclient against an attorney who failed to call and confirm the accuracy of the wire instructions are being upheld despite the lack of any traditional privity with the lawyer.

Despite the growing number of such claims, there is a noticeable absence of case law dealing with privity as a defense in wire scam cases. This likely occurs for two reasons. First, duty is not a required element of a contribution claim, which makes privity irrelevant. Second, such cases are being settled due to the lack of any viable defense, as failing to verbally confirm instructions before sending a wire is a given for attorneys and nonattorneys alike.

In addition to being exposed to nonclients, attorneys must be diligent with their errors and omissions insurance as well. Malpractice carriers are catching up to these situations, and many policies now exclude claims for wire fraud, leaving attorneys without insurance coverage to deal with typically very large damages.

Nevertheless, the historical protection of privity is not entirely gone, and some New York courts are protecting lawyers when a nonclient brings a legal malpractice claim against the attorney where wire fraud was involved — even where the attorney unwittingly sent the false instructions — but only where the attorney was not the party who should have called to verify the wire instructions.

In Contour Mortgage Corp. v. Reverse Mortgage Solutions Inc., the attorneys representing the purchaser's mortgage lender emailed all parties to obtain the final payoff letter just prior to the closing.[10] The seller's attorney emailed the real payoff instructions to the lender's attorney.

However, on the day of the closing, a fraudulent email was sent impersonating the seller's attorney, which contained fake payoff instructions. The lender's attorney failed to verbally confirm the wire instructions before sending the wire, and more than $350,000 was wired to the cyber scammer.

The nonclient lender brought a legal malpractice action against the seller's attorney, alleging that the firm breached the standard of care when it provided false, erroneous and fraudulent information in the payoff letter. The Supreme Court of the State of New York, County of Nassau, granted the defendant seller's attorney's motion to dismiss last May, holding that no privity existed between the parties.

The court held that the seller's attorney was not retained by and had no relationship with the purchaser's mortgage lender. Therefore, any claim for legal malpractice was meritless, according to the court. The court emphasized that the seller's attorney "was not the entity responsible for wiring or confirming receipt of any funds at all."

In First American Title Insurance Co. v. Liberty Land Abstract Inc., the title insurance company's title agent agreed to serve as the title closer, settlement agent and escrow agent in connection with a real estate transaction. At the closing, the seller's attorney provided the title agent with a payoff statement for the seller's mortgage.[11]

The title agent made a phone call to verify the information in the payoff letter but called the number on the false wire instruction instead of independently verifying the number before calling. Relying on the false instruction, the title agent issued a wire for more than $422,000 to the cyber scammer.

The purchaser filed a claim under its policy on the basis that the seller's mortgage was not paid off. The nonclient title insurance company then brought a lawsuit against the seller's attorney, alleging common law indemnification, negligence, and professional malpractice.

In 2022, the Nassau County Supreme Court granted the seller's attorney's motion to dismiss, holding that the seller's attorney did not share a special or near-privity relationship with the title agent or the title insurance company, and the seller's attorney did not undertake to verify the instructions.

Conclusion

Attorneys who become victims of email scams may find themselves defending claims for contribution brought by nonclients. These claims are not likely to be afforded the protection of a lack of privity.

Attorneys without a cyber policy may face these exposures without the benefit of an insured defense and indemnity. To avoid becoming a victim of email scams, the U.S. federal courts caution lawyers to never download attachments or click on links from unofficial or questionable sources.

Attorneys should pay careful attention to emails and be cautious of odd email addresses or unsolicited emails. It's also critical that attorneys vet wire instructions for a client's financial transaction — each and every time they send a wire. More importantly, attorneys must closely examine their insurance policies to determine whether they may be left out in the cold without coverage for these novel yet increasingly rampant claims.

Joseph Francoeur is a partner and national co-chair of the specialty professional risks practice at Wilson Elser Moskowitz Edelman & Dicker LLP.

Eve Soldatos-Mouzouris is of counsel at the firm.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Law Firm Cybersecurity Statistics, Konrad Martin, June 26, 2024; https://tech-adv.com/blog/law-firm-cybersecurity-statistics/.

[2] Why Law Firm Data Breaches Are Skyrocketing in 2024, Process Bolt, September 27, 2024; https://processbolt.com/insights/blog/why-law-firm-data-breaches-are-skyrocketing-in-2024/.

[3] Law Firms Five Times More Likely to be Targeted by Cyberattacks, Marissa Daily, TPX, January 17, 2025; https://www.tpx.com/blog/law-firms-five-times-more-likely-to-be-targeted-by-cyberattacks/.

[4] The Biggest Cyber Threats to Law Firms, Mike McLean, Embroker, August 5, 2024; https://www.embroker.com/blog/cyber-threats-to-law-firms/.

[5] Palm Ave. Hialeah Tr. v. Eisenberg, No. 24-cv-23586-BLOOM/Elfenbein, 2025 U.S. Dist. LEXIS 46855 (S.D. Fla. Mar. 13, 2025).

[6] Ferentini v. Mancini, Provenzano & Futtner, LLC, Docket No.: NNH-CV-21-6117046-S (Sup. Ct. J.D. of New Haven, March 13, 2025).

[7] Beware of Scam Emails Targeting Lawyers, The Florida Bar, Mark D. Killian, February 25, 2025; https://www.floridabar.org/the-florida-bar-news/beware-of-scam-emails-targeting-lawyers/.

[8] Electronic Filing Scam Targets Attorneys, The Federal Courts of the United States, November 6, 2024; https://www.uscourts.gov/data-news/judiciary-news/2024/11/06/electronic-filing-scam-targets-attorneys.

[9] Directive #11-23- Responding to Information Security Incidents, Including Compromised Attorney Accounts, Notices to the Bar, New Jersey Courts, July 3, 2023; https://www.njcourts.gov/notices/directive-11-23-responding-information-security-incidents-including-compromised-attorney.

[10] Contour Mortgage Corp. v. Reverse Mortgage Solutions Inc. et al., 605335/2022 (Sup. Ct. Nassau Cty. May 21, 2024).

[11] First American Title Insurance Co. v. Liberty Land Abstract Inc. et al., 600326-22 (Sup. Ct. Nassau Cty. July 25, 2022).