

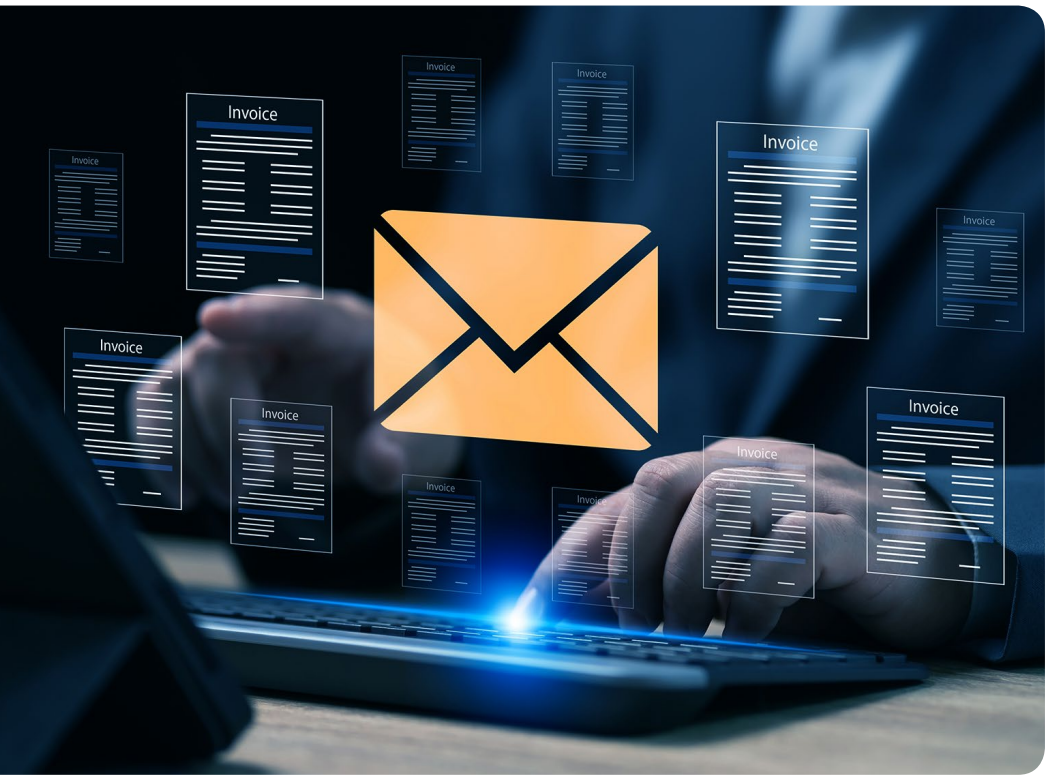
USI AFFINITY LEGAL ADVISORY

Hang Up and Call Back: Defending Your Firm Against the Luna Moth Help Desk Scam

USI AFFINITY

Prepared by Aaron M. Barham of the New York City-based law firm of Furman Kornfeld & Brennan LLP

Hang Up and Call Back: Defending Your Firm Against the Luna Moth Help Desk Scam



A criminal group the FBI calls the Silent Ransom Group, and security researchers call Luna Moth, has targeted U.S. law firms since the spring of 2023. The FBI issued a private industry notification about the group in May 2025 and a FLASH alert on May 26, 2026, after the group began impersonating law firms' own IT departments by phone. Mandiant reported in June 2026 that the group hit dozens of legal, financial, and professional services firms between January and May 2026, with data theft often complete within hours of first contact.

If you run a firm of five or fifty lawyers, assume you are in the target set. Your document management system may have the same deal files, tax returns, and Social Security numbers that a 500-lawyer firm's does. What you are less likely to have is a security team watching the network, a help desk with a verification script, and a receptionist who has been told what a fake IT call sounds like.

How the Attack Works

The attack has four steps.

- **The email.** A lawyer or staff member receives a phishing email styled as an invoice, a subscription renewal, or an "IT issue" notice. Some campaigns flood the inbox with junk subscription emails instead. There is no link and no attachment, so email security tools have nothing to flag.
- **The call.** Within minutes or hours, a phone call or external Microsoft Teams call arrives from someone claiming to be the firm's IT department or outsourced IT vendor. The caller references the email, knows the target's name, and walks the target into a remote session, then has the target install a remote management tool such as AnyDesk or Zoho Assist. These are legitimate products, so antivirus software does not object. The group registers lookalike domains such as [firmname]-helpdesk.com to make the request look internal.
- **The theft.** Nothing is encrypted. The group searches document management systems and cloud storage for client files, deal documents, tax records, and personal identifiers, then copies them out. In one incident Aon describes, the theft ran in small increments over two months and endpoint monitoring never alerted.
- **The extortion.** The ransom email can arrive within 30 minutes of the group leaving the network. It sets a short deadline, threatens to post the files on the group's leak site, and warns that the group will contact the firm's clients directly if the firm does not respond.

For targets that refuse the remote session, the FBI's May 2026 alert describes a fallback: the group sends a person

Continued on next page ▸

to the office claiming to be IT support, who says the computer needs to be imaged because of the phishing email and leaves with the data on a USB drive.

What Every Firm Should Do Now to Protect Itself

- **Make it a rule:** No remote access without a callback. Nobody at the firm grants remote access to a computer, approves a login prompt they did not initiate, or installs software at a caller's request until they have hung up and called the firm's IT provider back at a known number. Put the rule in writing and circulate it. The FBI's first recommendation to law firms is a written policy on how IT support contacts employees and authenticates itself.
- **Circulate who IT is.** Calling back only works if everyone knows who to call. Distribute the IT provider's name, the names of the technicians who service the firm, and the one number to use. Post it where the receptionist and office manager can see it. If a caller gives a name that is not on the list, the conversation is over. Ask the provider whether it ever cold-calls staff; if it does, change that.
- **Lock down remote access tools and USB ports.** The FBI recommends disabling remote access software and USB installation on computers that hold confidential data, so that no employee can install AnyDesk or plug in a drive without an administrator. Require phishing-resistant MFA (security keys rather than text codes) for partners and administrators.
- **Train for the call and the visitor.** Phishing training has focused on links and attachments; the group removed both. Cover the voice call, the Teams call, and the visitor who says he is from IT, and check identification before anyone touches a firm computer.
- **Write the incident plan before the incident.** Name the breach coach, the forensic vendor, and the one person authorized to communicate with a threat actor. Notify the carrier through the policy's incident-response channel before any negotiation or payment; the policy's consent requirements control. Report attempts, including near misses, to the local FBI field office or ic3.gov.

What the Rules Require

Comment [8] to Rule 1.1 of the *New York Rules of Professional Conduct* recognizes that competent representation includes keeping abreast of the benefits and risks of relevant technology. Rule 1.6(c) requires reasonable efforts to prevent unauthorized access to or disclosure of confidential information. Rules 5.1 and 5.3 require supervising lawyers to take reasonable measures to ensure that lawyers and non-lawyers at the firm conform to the Rules. The group often calls the



office manager or HR lead rather than a lawyer, so a firm with no written protocol for verifying IT requests has a supervisory gap before anyone picks up the phone.

A breach involving, or with a substantial likelihood of involving, material client information triggers a duty under ABA Formal Opinion 483 to notify affected clients. New York's SHIELD Act (General Business Law 899-aa) requires notice to affected New York residents and to the Attorney General and other state agencies when private information has been, or is reasonably believed to have been, accessed without authorization. Private information includes Social Security numbers, financial account, and driver's license numbers, biometrics, and health information. Other state statutes cover their own residents. Clients whose information was published will have claims available, and the firm's policies, training records, and IT vendor contract will be discovery targets.

Continued on next page ▸

Insurance Questions to Answer Before an Incident

- **Which policy responds.** A lawyers' professional liability policy covers claims arising from legal services, and many LPL forms now carry cyber exclusions or sublimits. Forensic costs, breach coaching, notification, credit monitoring, and extortion payments usually sit in a standalone cyber policy. A firm with only one of the two should know which gaps that leaves.
- **Social engineering and extortion terms.** The attack succeeds because an employee voluntarily grants access. Some cyber and crime policies treat a voluntary act differently from a hack, and social engineering coverage is often a sublimit well below the policy limit. Extortion coverage typically requires the carrier's consent before any payment and excludes payments to sanctioned parties.
- **Notice and panel requirements.** Cyber policies often condition coverage on using the carrier's panel breach coach and forensic vendor. A firm that hires its own consultant on day one may have forfeited reimbursement. The first call after discovering an intrusion should be to the broker.
- **The application.** Cyber applications ask whether the firm uses MFA, restricts remote access tools, and trains staff. Those answers are representations.
- **The IT vendor's coverage.** Know what errors and omissions and cyber coverage the outsourced provider carries and whether the services agreement contains an indemnity. An indemnity is worth what the balance sheet and policy behind it are worth.

Conclusion

The attack turns on one moment: a person at the firm deciding whether to let a caller into their computer. Every lawyer, paralegal, and receptionist should be able to repeat the rule that governs that moment: nobody gets remote access unless you are certain it is our own IT provider working on a known issue, and certain means you hung up and called them back. ■

Sources

- FBI FLASH-20260526-01, Silent Ransom Group Impersonating IT Personnel through Social Engineering (May 26, 2026)
- FBI Private Industry Notification, Silent Ransom Group Targeting Law Firms (May 23, 2025)
- Mandiant/Google Threat Intelligence, Ongoing Targeted Campaign Against U.S. Law Firms (June 5, 2026), as reported by BleepingComputer
- ABA Formal Opinion 483 (2018)
- Aon Professional Services Practice, "Hello, This Is IT": Attacking Professional Service Firms Through Microsoft Teams (April 2026)
- New York Rules of Professional Conduct, Rules 1.1, 1.6, 5.1, 5.3
- N.Y. General Business Law 899-aa (SHIELD Act)

This article was prepared by Aaron M. Barham of the New York City-based law firm of Furman Kornfeld & Brennan LLP. Aaron is part of a team of over 40 lawyers and paralegals devoted to the defense of attorneys and other professionals in malpractice and disciplinary matters, as well as the defense of construction and personal-injury accidents. For more information about the above topic or the author, please visit www.fkblaw.com.

We trust that the above article was useful and thought-provoking; however, please note that it is intended as a general guide and opinion only, not a complete analysis of the issues addressed, and readers should always seek specific legal guidance on particular matters.

About USI Affinity

USI Affinity is a national leader in designing malpractice insurance solutions for over 22,000 law firms nationwide. We specialize in insurance, like you specialize in a specific area of practice. USI Affinity offers a proprietary, comprehensive Lawyers Professional Liability program specifically designed to mitigate risk and close gaps in coverage.

For more information, visit www.usiaffinity.com/for-your-profession/lawyers/professional-liability.