fucile & reising | LLP

April 2020 Oregon State Bar Bulletin

The Human Dimension: Lawyers, Staff Play Critical Role in Fighting Tech-Enabled Scams

By Mark J. Fucile
Fucile & Reising LLP

Law firms have two things that thieves value: money and information. Criminal schemes aimed at one or the other are neither new nor novel. *In re Galasso*, 978 NE2d 1254 (NY 2012), for example, involved a law firm office manager who embezzled over $4 million from a firm trust account. Similarly, a classic account of 1980s Wall Street scandals describes a lawyer at a major New York law firm who provided advance information to an insider trading scheme on six significant deals before they went public—generating over $600,000 in illegal profits.[1]

What has changed in recent years, however, is thieves' increasingly sophisticated use of technology to steal both money and information from law firms. Although comprehensive statistics are hard to come by, a New York City Bar ethics opinion issued five years ago reported that email scams had stolen $70 million from lawyers nationally.[2] Similarly, hackers relatively recently targeted seven large New York law firms for information on potential mergers and acquisitions.[3] Although these illustrations come from New York, the Oregon State Bar and the Professional Liability Fund routinely issue alerts to Oregon lawyers warning about a wide variety of internet scams targeting lawyers here.

Because many of today's scams exploit technology, technology plays an equally central role in combating them. At the same time, law firms cannot be lulled into a false sense of security that defending against technology-enabled scams is solely the province of the firm's IT department or consultant. To the contrary, lawyers and staff play an absolutely critical role in defending their firms because many technology-related scams prey on our human reactions.[4]

In this column, we'll first focus on scams oriented around stealing money from law firms and then on information. With each, we'll initially survey common risks and then outline corresponding practical solutions.

Money

Some thefts from law firms are the equivalent of armed robbery—such as "ransomware" where criminals encrypt law firm files and then demand money in return for an electronic "key" to decrypt them.[5] Others are more like common street crime—such as "toner pirates" who impersonate a firm's copy vendor over the telephone to sell unsolicited printer supplies.[6] The former usually occurs when a seemingly legitimate link included in an email that an unsuspecting firm lawyer or staff member clicks on downloads malware encrypting the firm's files

throughout its network. The latter is often directed at busy lawyers who think they are dealing with the firm's actual vendor.

Having your own money stolen is bad. Having your clients' money stolen from your care is even worse because it can have significant regulatory and liability consequences.[7] A sophisticated scheme in this regard occurs when a lawyer is contacted by a new "client" with a collection matter in the lawyer's hometown. The lawyer contacts the debtor with information supplied by the client and the debtor quickly agrees to pay the balance due. The debtor follows with a check on a seemingly legitimate bank, which the lawyer deposits into trust. The client is pleased but would like its money quickly, so the lawyer issues a corresponding check out of trust before the debtor's deposit has cleared. Later, the debtor's check is returned as uncollectible. By this time, however, the client has cashed the firm's check—which cleared because other firm clients had money in trust. The "client" has disappeared with the money. In effect, the law firm has unwittingly assisted thieves in stealing the other clients' money that the firm was holding in trust.[8]

Schemes such as these often take perverse advantage of two increasingly common facets of law practice today. First, unlike even a few years ago, we may now only "meet" our clients or others we interact with electronically.

Unfortunately, thieves often exploit that electronic familiarity. Second, today's competitive market puts an accent on quick client service. Again, thieves exploit today's "speed" of practice by designing schemes that take advantage of the lack of time for reflection.

Confronting these risks involves both training and awareness. Training educates lawyers and staff about new and recurring threats. Awareness uses the training to recognize and deter the threats when they occur. Properly implemented, neither should either compromise the efficiency of electronic practice or sacrifice responsive client service.

While both training and awareness must adjust to threats as they emerge, several practical steps firms can take to meet recurring scams are:

- Train both lawyers and staff to be wary of any link or file they receive electronically. Unless it is both from a trusted source and is expected, they should not open it on a device connected to the firm's network. If it is from what appears to be a trusted source, but is not expected, they should independently verify with the source that it is legitimate.
- Train both lawyers and staff to be polite but appropriately skeptical about unexpected calls they receive from claimed service providers

seeking information about firm equipment, services and banking. Information should not be shared unless and until the identity and authority of the person calling has been verified.

- Funds should never be disbursed from trust until the corresponding deposit has cleared. "Cleared" in this context means more than simply your bank has accommodated your firm with a "provisional credit" that makes it appear on-line that the funds are "available" in your account. "Cleared" means your bank has actually received the funds involved from the check-writer's bank.[9]

This is not intended to be an exclusive list. Firms should regularly take advantage of the excellent resources available from the OSB and Professional Liability Fund to reassess their defenses in light of evolving threats.[10]

Information

One of our opening illustrations involved hackers who successfully penetrated several large law firms electronically to steal sensitive information on pending deals.[11] The hackers were able to compromise one of the law firms by obtaining employee log-in credentials, entering the network involved and planting spyware that allowed them to monitor the emails of key firm partners for market-moving information.[12] Although this could occur without human interaction, a

more common approach is through "phishing" emails—which fool unsuspecting users into providing their log-in credentials.[13] Therefore, beyond technology-based defenses such as strong passwords and "two-factor authentication," the same training of law firm lawyers and staff on an appropriate level of wariness toward any email including links applies with equal measure to those seeking log-in information.

Depending on the firm's practice, thieves may be seeking information about the firm's clients or the firm itself. Firms doing business acquisitions like our opening example may be targets for thieves seeking client information to profit in the stock market. By contrast, firms carrying large trust account balances, such as the law firm in another of our opening examples, may be targets for thieves seeking banking information as part of an effort to steal funds being held by the firm. Although potential regulatory and liability consequences vary with what is stolen and from whom, none of them are "good."[14]

Beyond the firm's office, lawyers and staff should also be cautious when using mobile devices in public settings where they could be viewed or overheard. Using electronic security measures such "virtual private networks" instead of open public wi-fi and activating built-in device security features such as passwords, hard-drive encryption and remote "kill switches" are essential. Often

equally important to protecting confidential information, however, are simple steps like positioning laptop screens so they will not be seen by "prying eyes" and limiting conversations so they will not be overheard by "nosey neighbors."

Summing Up

The U.S. Department of Homeland Security has described thieves' use of human behavior to further technology-enabled schemes as a form of "social engineering."[15] Given that human dimension, lawyers and staff continue to play a vital role in protecting their clients and their firms from technology-exploiting schemes.

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP handles professional responsibility, regulatory and attorney-client privilege issues for lawyers, law firms and corporate and governmental legal departments throughout the Northwest. Mark has chaired both the WSBA Committee on Professional Ethics and its predecessor, the WSBA Rules of Professional Conduct Committee. Mark is a member of the Oregon State Bar Legal Ethics Committee and the Idaho State Bar Section on Professionalism & Ethics. Mark writes the Ethics Focus column for the Multnomah (Portland) Bar's *Multnomah Lawyer*, the Ethics & the Law column for the WSBA *Bar News* and is a regular contributor on legal ethics to the WSBA *NWSidebar* blog. Mark is a contributing author/editor for the current editions of the OSB Ethical Oregon Lawyer, the WSBA *Legal Ethics Deskbook* and the WSBA *Law of Lawyering in Washington*. Before co-founding Fucile & Reising LLP in 2005, Mark was a partner and in-house ethics counsel for a large Northwest regional firm. He also teaches legal ethics as an adjunct for the University of Oregon School of Law at its Portland campus. Mark is admitted in Oregon, Washington, Idaho, Alaska and the District of Columbia. He is a

graduate of the UCLA School of Law. Mark's telephone and email are 503.224.4895 and Mark@frllp.com.

---

[1] James B. Stewart, *Den of Thieves* 145 (1991).

[2] New York City Bar Formal Opinion 2015-3 at 1 (2015).

[3] *See* Leslie Picker, *3 Men Made Millions by Hacking Merger Lawyers, U.S. Says*, NY Times, Dec. 28, 2016, at B1.

[4] This column focuses on thefts by outsiders using technology. Firms should not overlook trust account and practice management addressing "old fashioned" thefts of either money or information by personnel within their firms. *See generally* Mark J. Fucile, *The Bookkeeper Did It! Lawyer Responsibility for Staff Theft of Client Funds*, 25, No. 2 ABA Prof. Lawyer 30 (2018).

[5] Robert Ambrogi, *Ransomware Attacks Hit Three Law Firms in Last 24 Hours*, Feb. 1, 2020, available at www.lawsiteblog.com; *see also* Nathaniel Popper, *Ransomware Attacks Grow, Crippling Cities and Businesses*, NY Times, Feb. 10, 2020, at B1.

[6] *See, e.g.*, Iowa Department of Justice, *Miller Files Consumer Fraud Lawsuit Against Alleged California "Toner Pirates*," Sept. 1, 2016, available at www.IowaAttorneyGeneral.gov.

[7] *See, e.g.*, RPC 1.15-1 (duty of safekeeping client property).

[8] This is a variant of a scheme described in New York City Bar Formal Opinion 2015-3.

[9] *See generally* Sylvia E. Stevens, *Waiting for 'Go' Dough—A Primer on Disbursing Client Funds*, 66 Or. St. B. Bull. 21 (June 2006).

[10] *See, e.g.,* Rachel Edwards, *Cybersecurity and Employee Training*, PLF inBrief (June 2019).

[11] *See* Note 3, *supra*.

[12] *Id.*

[13] The U.S. Department of Homeland Security defines and discusses "phishing" at: https://www.us-cert.gov/report-phishing.

[14] Under RPC 1.6(c), we have a regulatory duty to take reasonable measures to protect client confidential information from "unauthorized disclosure[.]"

[15] *See* Note 13, *supra*.