UnionBank®
The Private Bank

Financial Focus

Law Firm Fraud: Is Your Firm at Risk?

Each year, law firms around the country are collectively scammed out of millions of dollars. Will you be one of them?

From California to Florida and every state in between, the news headlines are strikingly similar: "Local law firm falls victim to cashier's check scam." And while it may sound like something you read in the paper ten years ago, it could just as easily have been this morning's story. This con has stood the test of time for one simple reason: Lawyers continue to fall for it.

The Set Up

Here's what typically happens: An attorney receives what appears to be a legitimate solicitation email from a potential client, who claims he is owed a large sum of money and would like to retain the attorney's services to recover it. Often he will say that he was referred to the attorney by a familiar party. He and the attorney reach an agreement regarding service terms and fees.

Shortly thereafter, the client purports that his debtor has been intimidated into paying up, and the attorney receives a seemingly valid cashier's check from a reputable bank for the large sum in question. The client authorizes the attorney to withdraw his fee and requests that the remainder is wired to his account, typically overseas. The attorney complies, only to realize too late that the check was fraudulent and the firm has handed over its money to a vanishing crook.

One recent example involved a high-profile firm based in Orlando. After being duped by an individual claiming he was owed money in a wrongful termination suit with his former employer, Kaufman, Englett and Lynd, PLLC lost the $285,000 they wired to a Japanese bank account.[1] Unfortunately, a quick Google search reveals dozens more stories just like this.

The Variations

The cashier's check scenario is just one example of how criminals prey upon law firms: Phishing emails and malicious software are also prevalent. Earlier this year, North Carolina firm Wallace & Pittman lost $336,000 with the click of a mouse when a link within a valid-looking email about a recent ACH transaction enabled hackers to install key-stroke-tracking software on an employee's computer. This revealed the firm's banking passwords and allowed the thieves to wire funds to a Russian bank account. To make matters worse, the firm is now involved in a lawsuit with their bank over who is responsible to carry the loss.[2]

The Federal Bureau of Investigation (FBI) also reports a rise in cyber attacks targeting sensitive client data, including everything from patent applications to company merger details.[3] The same modern technology that makes it easier to conduct everyday business—shared servers, virtual document storage, thumb drives, etc.—has also made it easier for hackers to access any and every piece of information they desire once they break into your network.

The Temptation

It's easy to read about scams on paper and wonder how anyone could be so foolish as to fall for them. But in the heat of the moment, when you are faced with the reality of a sagging economy and the pressure of obtaining new clients, it's even easier to let your guard down. In the quest for more billable hours, a sizeable retainer fee on a freshly minted cashier's check may seem like a great opportunity.

Furthermore, increasingly sophisticated tactics make it difficult to discern between legitimate and fraudulent documents. Particularly vulnerable are small firms and sole practitioners, who may lack the training and resources necessary to protect the large volume of sensitive data they store.

The Defense

Perhaps the most troubling aspect of this growing trend is that once you realize you have fallen victim to fraud, it's almost always too late to do anything about it. Cyber criminals

are rarely caught, and banks are rarely held responsible for fraudulent transfers. Therefore, the key to protecting yourself is prevention. The following tips will help you learn to recognize suspicious activity and protect sensitive information so you can stop fraud before it happens.

- **Promote awareness** – Ensure that everyone in your office—from attorneys to administration to accounting—is aware of the threat of fraud. When handling cashier's checks, remind your staff to be on the lookout for signs of forgery and to contact the check's issuing financial institution for verification. Do not use the telephone number on the check, as it may be phony. Obtain the issuer's contact information from another source.
- **Know your client** – These days, it's very possible to have a legitimate attorney-client relationship where you have only met with a client by email or phone. Consider it a warning flag, however, and be extra vigilant about confirming all information provided by such a client. This includes contact information, business relationships and any third parties mentioned—especially references.
- **Don't jump the gun** – Never rush to disperse funds by wire transfer, particularly from your trust account, and especially to an apparently unrelated third party offshore. If the client is impatient and pressuring you to send funds immediately, you can almost bet you're dealing with a scammer. Always wait for the check to clear. Keep in mind, however, that "cleared" can be an ambiguous term. As a courtesy, many banks make funds available to customer accounts before a deposited item is actually paid by the payor bank. To be on the safe side, call your bank for clarification.
- **Follow online security best practices** – Remember that cyber criminals attack silently and without warning. Key areas to focus on fortifying include:
  - **Segregation** – Dedicate one laptop or desktop computer for banking transactions only. Do not use it for any other purpose, and do not conduct banking transactions on other devices.
  - **Passwords** – Have a password consisting of nothing more than eight lowercase letters? It would take a hacker an average of just two hours to guess it.[4] The more variation you add in the form of uppercase letters, numbers and symbols, the longer it would take to crack. You also want to make sure to change your passwords every 90 days, never use the same password twice, and never keep them stored near computers or sensitive records.
  - **Encryption** – Stolen laptops, lost thumb drives and vulnerable backup systems are the leading sources of data breaches. Be sure these and wireless networks are encrypted.
  - **Software** – Every desktop computer, laptop and mobile device should be equipped with firewall, anti-virus, anti-spyware and anti-spam software. For best results, use one single integrated product across the board.
  - **Server room** – Your server room should be kept locked at all times.
  - **Employees** – When a staff member is terminated or resigns, immediately delete that person's online credentials and sever all possible network access, including remote.

The Bottom Line

It bears repeating: The only truly effective way to protect your firm from the detrimental aftermath of fraud is to prevent it. Institute official office policies concerning things like the handling of cashier's checks and online security measures. Make them readily available in black and white, train your staff on them at least once per year and reference them often in staff meetings and employee reviews.

Above all else, practice common sense and trust your instincts. If a transaction feels suspicious or sounds too good to be true, it probably is.

Contact your Relationship Manager for more information.

Notes

1 "Feds: KEL law firm scammed out of $285K," Amy Pavuk, *Orlando Sentinel*, Jan. 19, 2012, http://articles.orlandosentinel.com/2012-01-19/news/os-kel-law-firm-scammed-20120119_1_kel-englett-and-lynd-bank-account, accessed June 7, 2013

2 "Law firm fell victim to phishing scam, precipitating $336K overseas wire transfer, bank suit alleges," Debra Cassens Weiss, *ABA Journal*, April 4, 2013, http://www.abajournal.com/news/article/law_firm_fell_victim_to_phishing_scam_precipitating_336k_overseas_wire_tran, accessed June 7, 2013

3 "Why are Cyber Attacks on Law Firms Such a Significant Threat?" Trey Tramonte, eDiscoveryInsight.com, March 15, 2013, http://ediscoveryinsight.com/2013/03/why-are-cyber-attacks-on-law-firms-such-a-significant-threat, accessed June 7, 2013

4 "E-Security Pros Offer 15 Tips to Help Law Firms Better Protect Sensitive Data," John W. Simek and Sharon D. Nelson, Oregon State Bar, Oct. 2012, http://www.osbar.org/_images/bulletin/12oct/Esecurity.pdf, accessed June 12, 2013