How to protect client funds from hackers

大成 DENTONS

February 9, 2016

"*Legal representation based on breach of sale contract. I wait to hear from you if your firm take on sure case. Just click this link for more information about the case and the rates we will pay! Kind Regards, Iam ScamArtist*."

Have you seen an email like this? Typically, it is sent from someone that neither you nor anyone at your firm has ever heard of.

These types of messages are one of a number of scams that are hitting attorneys every day. This scam attempts to gain access to law firm accounts, including escrow accounts, with Trojan horses, viral missiles and greenmail attacks.

Traditionally, attacks on attorney trust accounts consisted of three major types of frauds: (1) counterfeit bank checks; (2) forged trust account checks; and (3) desperate or dishonest attorneys or non-attorney staff abusing their access to the accounts.

Recently, though, trust account thefts have become much more sophisticated. They involve elaborate electronic missives that invade law firm computer systems and lock in on passwords for access codes and account numbers. When these thefts are successful, the attorneys and law firms may be left to make up the difference.

For example, in 2010, a solo practitioner in Florida found that $35,000 was stolen from her firm's trust account by a hacker. Similarly, in December 2013, a Toronto-area law firm suffered from a six-figure loss after a hacker used a computer virus to access the computer of the firm's bookkeeper.

So what happens when a cybersecurity event implicates a firm's trust account? Are lawyers liable when a computer hacker steals client funds?

The State Bar of California has addressed the issue of stealing when the culprit is an employee of the attorney or firm. For instance, in *In re Malek-Yonan*, several members of a firm's non-attorney office staff stole approximately $1.7 million from the client trust account, using their apparent authority as employees. The attorney had no knowledge of the theft and attempted to reimburse all clients. There, the Review Department of the State Bar Court of California disciplined the attorney not for misappropriation of client funds, but for gross negligence in failing to have adequate office procedures and to provide adequate supervision for staff—which ultimately lead to the theft of client funds.

Most state bar associations, including the State Bar of California, have not yet addressed whether an attorney is liable when *an independent* third party, rather than an employee, steals client funds. However, just last July, the North Carolina State Bar addressed several inquiries regarding the professional responsibility of an attorney when a third party not employed or supervised by the attorney has stolen funds from the attorney's trust account. See N.C. State Bar, 2015 Formal Ethics Opinion 6, "Lawyer's Professional Responsibility When Third Party Steals Funds from Trust Account."

The North Carolina Ethics Committee noted that the attorney generally will not be professionally responsible for

replacing funds stolen from the trust account—so long as the attorney was otherwise managing the trust account in compliance with the applicable Rules of Professional Conduct.

The committee noted, though, that the result might be different if the attorney failed to follow the Rules of Professional Conduct on trust accounting and supervision of staff, and that failure was ultimately the proximate cause of theft from the trust account. In such a situation, the North Carolina committee concluded that the attorney might be responsible for reimbursing the trust account.

Of course, this recent North Carolina opinion begs the question of what exactly the Rules of Professional Conduct require for reasonable steps for supervising and protecting client escrow funds, especially when the world of the Internet is changing so rapidly. There are some lessons that can be learned from situations that have already happened.

First, attorneys must take care to ensure compliance with all rules governing client trust fund accounts. Rule 4-100 of the California Rules of Professional Conduct sets forth the minimum standards for preserving client funds and property. In essence, Rule 4-100 requires that an attorney maintain a separate designated account for client funds and that an attorney maintain sufficient records to keep track of how much money is held for each client at all times. An attorney must be sure to use the funds of a particular client to satisfy the obligations of another client.

Section (C) of Rule 4-100, which refers to specific standards from the Board of Governors of the State Bar, provides those specific minimum records—such as a client ledger and account journal—that are mandatory for a firm's trust account. This section also requires that an attorney reconcile the trust account every month and maintain a written journal of transactions for a five-year period.

Attorneys who engage in online banking should consider taking steps to educate their partners and staff as to the myriad of security risks that may arise as a result of that approach and the protocols and protections in place to protect again third party theft.

Many law firms combat this thievery through employing strong password policies and procedures, using of encryption and security software, hiring of an information technology consultant, and training of both attorney and non-attorney staff members.

Such training could involve instruction on how attorneys and staff could spot or detect high-risk emails. Such emails could contain viruses that shut the system down absent the payment of a ransom.

Bogus emails can imitate legitimate emails in an attempt to learn usernames and passwords. And emails can invade systems as if the sender was an authenticated user. Seeing what these emails look like, how they operate, and the risks they pose are helpful for both attorneys and staff to actually see.

If client funds are misappropriated, regardless of whether an attorney believes that he or she is responsible for reimbursing the trust account, it is recommended that the attorney take certain steps.

First, upon discovering that client funds may have been compromised, best practices dictate that the attorney hire counsel specializing in cybersecurity and law firm defense issues. The early moments after a hacking incident will feel chaotic: there are a number of fires that need to be put out and a growing number of issues that will need immediate resolution. Hiring experienced specialty counsel will help handle these mounting issues while also preserving and maintaining privilege.

Any perception that a law firm is not taking adequate steps after discovery or that it is acting in its own interests may damage the firm's reputation. Hiring outside counsel immediately reflects extra due diligence in addressing a problem and shows the law firm's dedication to fulfilling its ethical and legal obligations.

If client funds appear to be missing from a law firm trust account, attorneys should promptly investigate the cause of

the stolen funds and take steps to prevent any possible further thefts, including, for example, considering whether it is appropriate to close the trust account and transfer the funds to a new account.

Time is of the essence with hacking issues. An unaddressed breach inevitably expands until detection, causing greater exposure and more scrutiny of the firm's oversight of client funds.

Identifying notification obligations under federal and state laws is critically important. In many situations, Internet-related hacking is a crime. California was the first state to enact a data breach notice law in 2003, requiring a business to notify any California resident when unencrypted personal information is, or is reasonably believed to have been, acquired by an unauthorized person. See Cal. Civ. Code §§ 1798.29(a), 1798.82(a). This duty of notice is triggered only when certain personal information, such as Social Security numbers or financial account numbers, may have been compromised. Still, this law pinpoints that law firms, like other businesses, may have a duty to report cyber hacking. In this regard, law firms also need to determine whether and to what extent authorities should be involved in such a matter.

In all situations, an attorney has a duty to notify the clients of the theft and to advise the clients of any consequences for representation. The attorney should also help the clients identify any source of funds, such as bank liability and insurance, to cover their losses.

The attorney should also be sure to provide timely, prompt notice to all insurers.

Though cybersecurity becomes more difficult as methods of hacking progress, being mindful of client trust accounts and following these early steps in the event of a breach will minimize the exposure for both the firm and its clients.

As published by *The Recorder*

Your Key Contacts

Shari L. Klevens
Partner, Washington, DC
D +1 202 496 7612
shari.klevens@dentons.com