CNA

PROFESSIONAL COUNSEL℠

ADVICE AND INSIGHT INTO THE PRACTICE OF LAW®

Alert: New Scam Targeting Lawyers Wiring Funds

Lawyers should beware of a sophisticated new hacking scam the FBI refers to as "Business E-mail Compromise." Lawyers in multiple states have recently reported being victimized by this scam. The hoax targets lawyers who process client funds from their attorney trust accounts. Transactions involving real estate closings or legal settlements are vulnerable to this ploy. Typically, the hacker will impersonate the intended recipient of a payment via e-mail communications and manipulate the lawyer into wiring client funds to a fraudulent bank account. After the funds are fraudulently transferred, the lawyer may be obligated to replace the lost client funds.

Details of the Scam

The scam proceeds as follows: first, a criminal hacks into a lawyer's e-mails and monitors the lawyer's e-mail traffic in an undetected manner. Eventually, the criminal learns that the attorney will be making a wire transfer of client funds relating to a settlement or transaction. The criminal then creates a "spoof" e-mail address that is almost identical to the e-mail address of the intended recipient of the funds. For example, the fraudulent e-mail address may be the same as the intended recipient's e-mail address, except for one character. Using this fraudulent e-mail address, the criminal e-mails the attorney and requests that the attorney wire the funds to a bank account in the United States.

The scam ultimately depends upon the lawyer failing to follow up with the actual intended recipient to confirm the instructions in the fraudulent email. If the lawyer were to contact the true recipient prior to following the emailed instructions, then the fraud would be discovered. However, the lawyer may reasonably rely upon the emailed instruction as emails may represent a customary means of communication in the deal.

If the attorney does not discover the fraud, then the lawyer wires the money to the sham bank account. Typically, the bank account belongs to an innocent party who has been instructed to open the account in order to receive wire funds. The criminal has told this individual that he or she simply must wire the funds to a foreign bank, and he or she can then retain 10% of the funds for his or her trouble. Following these instructions, the funds are then wired to the foreign bank, rendering the funds unrecoverable.

The criminal continues to perpetrate the scheme by creating a fraudulent e-mail address based upon the attorney's own email. The criminal then sends e-mails to the true intended recipient of the funds, purportedly from the attorney, providing an excuse as to why the funds had not yet been delivered. The excuse often involves a fabricated family emergency or other personal loss. As a result, the intended recipient of the funds may delay several days before contacting the attorney. By the time the intended recipient telephones the attorney, all but 10% of the funds have been transferred out of the country. The intended recipient inevitably demands satisfaction from the lawyer, who no longer has access to the client's funds and must use his or her personal resources to compensate the client for the difference.

Ethical and Legal Concerns for Lawyers

This scam has significant ethical and legal implications for lawyers. First, by failing to preserve client property, the lawyer may violate Model Rule of Professional Conduct 1.15 ("Rule 1.15"). Under Rule 1.15, lawyers have obligations of safeguarding, accounting and delivery when holding the money or property of others. Rule 1.15 does not expressly include an intent element and some authorities have suggested that no intent need be proven to establish a violation.[1]

Most state bar associations have not yet directly addressed whether a lawyer is liable when a third party not employed or supervised by the lawyer steals client funds. The North Carolina State Bar was the first to address this question in an October 2015 ethics opinion.[2] According to the Opinion, lawyers are required to use reasonable care to prevent third parties from gaining access to client funds held in the trust account.[3] As a result, a duty is imposed upon the lawyer to implement reasonable security measures, such as telephoning the intended recipient of the funds at the phone number listed in the lawyer's file or confirming the intended recipient's e-mail address.[4] In addition, the lawyer has affirmative duties to "educate himself regularly as to the security risks of online banking; to actively maintain end-user security at the law firm through safety practices such as strong password policies and procedures, the use of encryption and security software, and the hiring of an information technology consultant to advise the lawyer or firm employees; and to insure that all staff members who assist with the management of the trust account receive training on and abide by the security measures adopted by the firm."[5]

Notably, the Opinion concludes that when a lawyer fails to take reasonable care to minimize the risks to client funds by implementing reasonable security measures, the lawyer may be found professionally responsible and may be required to replace funds stolen by the criminal.[6]

Risk Management Tips

Increasingly, hackers are targeting law firms due to their access to client funds and valuable client information. Lawyers who engage in online banking thus have an affirmative duty to educate themselves and their staff on the relevant security risks and also ensure that they employ the necessary security precautions to prevent third party thefts.

In addition, a lawyer or law firm employee may unknowingly expose his or her law firm to a virus. Once a virus is present on the firm's computer, hackers may be able to obtain back door access to the law firm's most sensitive information. Therefore, both lawyers and staff should receive training on detecting high risk e-mails. Suspicious e-mails should not be opened and should be deleted immediately. If a suspicious e-mail is opened, the lawyer should neither reply to it under any circumstances, nor click on any links within the e-mail. Most importantly, lawyers should not install and download any software from the Web before first confirming that they are working with a trusted source.

It is also critical to recognize that unencrypted e-mail is not a secure mode of communication for lawyers. When sending confidential information via e-mail, lawyers should use e-mail encryption technologies.

Other important security precautions for law firms include the following:

- Install a personal firewall and an anti-virus program and keep them running at all times.
- Ensure that the firewall and anti-virus program are updated automatically.
- Install security patches for Windows and Microsoft Office programs immediately, and enable automatic updates.
- Adjust the security settings in your Web browser to the maximum protection level while simultaneously permitting the firm to use its browser as needed.
- Implement strong password policies and procedures.

1 See *In re Mayeaux*, 762 So.2d 1072 (La. 2000)("lawyer's mistake, good faith, or lack of conscious wrongdoing does not negate an infraction of the rule"); *Att'y Grievance Comm'n v. Stolarz*, 842 A.2d 42 (Md. 2004)("an unintentional violation…is still a violation of the attorney's affirmative duties imposed by the rule"); Restatement (Third) of the Law Governing Lawyers §5 cmt. (d)(2000).
2 See FEO 6, The North Carolina State Bar, October 23, 2015.
3 *Id.*
4 *Id.*
5 *See* 2011 FEO 7, The North Carolina State Bar, 2011; 2015 FEO 6, The North Carolina State Bar, October 23, 2015.
6 *See*, e.g., 2015 FEO 6, The North Carolina State Bar, October 23, 2015.

Before wiring client funds, lawyers always should initiate a phone call, to a number known to be valid, rather than a number referenced in an e-mail), to confirm the wiring instructions. Be especially cautious about any sudden and emergency changes to prior wire instructions.

If it appears that client funds have been stolen, law firms must act immediately to investigate the breach and prevent further thefts. Professional advisors, including legal counsel, specializing in cybersecurity or professional liability issues should be retained to provide guidance on potential sources to cover the firm's losses, as well as on any ethical and legal obligations the lawyer may have following the theft.

Conclusion

Lawyers are required to use reasonable care to prevent third parties from accessing client funds held in the trust account. Never wire funds based merely on an e-mail communication – always telephone the number in the client file to confirm the wiring instructions, even if a different number is provided via e-mail. By implementing proactive measures, lawyers can significantly reduce their exposure to a hacking scam.

CNA

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com.