The Hanover Insurance Group®

Hanover Lawyers Professional Advantage

Risk Bulletin: Email Wire Fraud Scam Affecting Lawyers and Law Firms

LAWYERS WHO WIRE MONEY TO OR ON BEHALF OF CLIENTS SHOULD BE AWARE OF RECENT WIRE FRAUD SCAMS

Lawyers who wire money to or on behalf of clients should be aware of a fraud scheme that could potentially cost the lawyer and/or client hundreds of thousands of dollars. In the United States alone, the Federal Bureau of Investigation (FBI) reports that as much as $750 million have been lost to wire fraudsters[i].

While wire fraud scams affect many different types of professionals, lawyers who work with real estate clients and/or wire funds as part of their practice are particularly vulnerable. To help lawyers manage their risk, we have highlighted the typical scenario and provided risk management guidance to avoid becoming a victim of a fraud scheme.

A. Typical Wire Fraud Scam Scenario Faced by Lawyers

The scam typically involves a compromised email account from one or more parties to a real estate or commercial transaction[ii]. The FBI refers to this scam as the "man-in-the-email-scam.[iii]" The scammer assumes the identity of a party to the transaction and uses an email address that appears to be from the legitimate sender. It could be an email from the "purported" real estate agent, mortgage broker, seller's attorney, etc. The scammer may even have control over the person's real email address or the email may use a similar, but slightly altered domain name (e.g., john@attorney.**us** (changing domain name suffix) or John@att**0**rney.com (changing a letter "o" to a number "0" in the domain name) instead of john@attorney.**com**)[iv]. With control over a person's real email address, the scammer can obtain knowledge specific to the transaction, information about all the parties to the transaction, various timetables, etc.

The scammer has usually already had enough access to previously exchanged emails in the transaction to seem convincing to the attorney receiving the email (e.g., "I hope the home inspection went well yesterday"). The scammer will typically provide wire instructions or make some change to a previous wire transfer request. Sometimes, the scammer may even change the transaction details, such as account numbers or changing the original plan of having payment made by check to requiring payment via a wire transfer.

To circumvent normal channels that might uncover a fraud, the scammer will emphasize that "time is of the essence," and that this matter is "urgent." Typically, the scammer will use common

continued ▸

business phrases such as "this needs to go out today," "I need you to take care of this ASAP," "client is impatient" and/or the "seller may pull out if action not taken care of immediately," etc.

The attorney will then wire out the money for the closing which can be hundreds of thousands of dollars to the scammer's account. The money is quickly transferred by the scammer to an overseas bank before the scam can be uncovered and stopped. The real party often calls late in the day or early the next morning asking the attorney what happened to the anticipated wired funds.

B. Potential Damages

At that point, the attorney realizes that he or she has been scammed. The closing cannot take place and various claims for damages can accrue as a result of the failed sale of property (other party to the transaction) as well as a claim for the loss of the client's funds. Thus, there are usually at least one or more aggrieved parties looking to the attorney for their actual damages, plus any additional attorney's fees and costs incurred by all the aggrieved parties in trying to rectify the situation.

Other potential damages from the fraud

In addition, depending on the nature of the scam, the funds placed into an attorney's client trust account can be fraudulent as in the case of the check fraud scam[v]. If the funds wired from the attorney's client trust account turn out to be fraudulent, the attorney also faces the problem of having withdrawn other client's or clients' funds from the trust account. The attorney may be exposed to professional liability claims by those clients for the missing funds. Worse, the attorney may also face potential disciplinary action for the misuse or misappropriation of client funds.

C. What to Do if Faced with a Wire Fraud Scam

When an attorney realizes he or she has been the potential victim of a wire fraud scheme, the attorney must act immediately since time is of the essence when trying to identify the fraudulent parties (scammers) and/or recover any of the funds. The attorney should immediately call all affected clients, parties and financial institutions involved in the transaction. The bank entities have been occasionally successful in blocking or recovering some or all of the wired funds.

Additionally, the attorney should contact both the local police and the FBI and follow any reporting requirements and suggestions required. Attorneys can submit all relevant info to the Internet Crime Complaint Center (IC3) at www.ic3.gov.[vi] While coverage is not a given, attorneys should report all claims or potential claims to their insurance carriers who issued insurance policies that may provide coverage.

D. Avoiding and Managing the Risk of Wire Fraud Scams[vii]

i. **Be Skeptical**
First, attorneys need to be on the lookout for wire fraud scams and exercise a healthy dose of skepticism whenever money is being wired to complete a transaction of any kind. Wire fraud scams utilizing emails can involve anyone in a transaction, from someone the attorney has known professionally for 40 years to someone they have only known for a short time through one transaction. The nature of email practice can shield the true identity of the individual much more easily than through a transaction involving the exchanging of information via the telephone or in person.

ii. **Employ Second-Factor Authentication via Telephone Calls Prior to Wiring Funds**
Before any money is ever wired out of the law firm for a transaction, an attorney can uncover most potential fraud scams by merely calling the person who is purportedly sending the email. Attorneys should always use the previous contact info they have for the person rather than contact info contained in the potentially fraudulent email. Attorneys can also call someone else at the company. The main point is to take action outside of the potentially hacked email chain.

iii. **Be Wary of Last Minute Changes in Business Practices**
Be wary when a party in a transaction suddenly changes their normal procedures. This could include wiring money to a different account, using a personal instead of a work email address, or contacting a different person at the company. All of these could be red flags to a potential scam. The best method to be careful is to use

second-factor authentication described above to confirm the proposed change.

iv. **Utilize Email Security Measures**
Attorneys can minimize their risk by using simple email security measures. First, to the extent possible, attorneys should use digital signatures or other encrypted email tools. Do not open spam email (unsolicited) or click on any links or open attachments in spam email. Delete spam email immediately.

For business purposes, attorneys should avoid the use of free, web-based email programs such as Gmail and/or Yahoo. It is safer to establish a company website domain and use it to establish company email accounts. To the extent financially possible, attorneys and firms should purchase near-identical spellings and versions of the firm domain name to prevent fraudsters from using those similar domain names to further their fraud scams (e.g., purchase lawfirm.com as well as lawfirm.org, lawfirms.com, lawfirms.org, etc.)

Attorneys should not use the "Reply" option to respond to any business emails. It is better to use the "Forward" option and either type in the correct email-address manually or select it from the attorney's previously stored contact info for the recipient. This technique ensures that the correct email address is used although it may not frustrate a fraudster who has taken over a recipient's email account.

v. **Use Computer Security Experts**
Attorneys should consult with computer safety and information technology experts and make sure that their firm is up to date on all virus and hacking protection software.

vi. **Train All Employees including Firm Administrators**
Attorneys need to train all employees at the firm, including firm administrators, paralegals, and assistants on the potential for fraud scams and discuss the risk management techniques available to best manage the risk. Require all employees to utilize second-factor authentication.

vii. **Other Risk Management Techniques**
Fraud scams perpetrated on attorneys are constantly evolving and changing. Be ready for a potential fraud to reveal itself in a different scenario or format than discussed in this article. Stay aware of current internet scams. Attorneys can review common scams seen by the FBI by visiting http://www.fbi.gov/scams-safety/frauds-from-a-z and learn about techniques to reduce their risk of being scammed: http://www.fbi.gov/scams-safety/fraud/Internet_fraud.[viii]

E. Conduct Coverage Check

Last, insurance coverage for such wire fraud scams is not a given under a variety of potential insurance policies and endorsements, including but not limited to, professional liability, general liability, fidelity, privacy breach, directors & officers, employment practices and cyber policies. There may also be partially uncovered or excluded claims and/or damages even if there is coverage for other aspects of the fraud scheme. Attorneys should discuss their coverage for these types of scenarios carefully with their agents as to what their policies may cover or exclude.

F. Conclusion

By making themselves aware of potential scams in any scenario where funds are being wired, attorneys can go a long way to avoid becoming the victim of a costly and professionally troublesome fraud scheme.

The recommendation(s), advice and contents of this material are provided for informational purposes only and do not purport to address every possible legal obligation, hazard, code violation, loss potential or exception to good practice. The Hanover Insurance Company and its affiliates and subsidiaries ("The Hanover") specifically disclaim any warranty or representation that acceptance of any recommendations or advice contained herein will make any premises, property or operation safe or in compliance with any law or regulation. Under no circumstances should this material or your acceptance of any recommendations or advice contained herein be construed as establishing the existence or availability of any insurance coverage with The Hanover. By providing this information to you, The Hanover does not assume (and specifically disclaims) any duty, undertaking or responsibility to you. The decision to accept or implement any recommendation(s) or advice contained in this material must be made by you.

i. *Hackett, Robert, "How This CEO Avoided Getting Conned in a Wire Fraud Scam," Fortune, October 13, 2015.*

ii. *Note there have been earlier versions of the wire fraud scam affecting lawyers since at least 2006 typically involving hard copies of cashier's checks that take advantage of an attorney's lack of knowledge with UCC Codes and bank regulations involving when funds are available and when a check has been fully cleared.*

iii. *Dietrich-Williams, Ayn, "'Man-in-the-E-Mail' Fraud Could Victimize Area Businesses," FBI Seattle, December 2, 2013.*

iv. *Scammers can also change the name in the email address without changing the domain name (e.g. j0hn@attorney.com (changing letter "o" to numeral "0" instead of john@attorney.com.*

v. *See infra note ii.*

vi. *See infra note iii.*

vii. *Ibid.*

viii. *Ibid.*

Why The Hanover?

The Hanover is a leading property and casualty insurance company dedicated to achieving world-class performance. Our commitment is to deliver the products, services, and technology offered by the best national companies with the responsiveness, market focus, and local decision making of the best regional companies. This powerful combination has been a proven success since our founding in 1852, and all insurance company subsidiaries are rated "A" (Excellent) by A.M. Best Company.

The Hanover Insurance Group®

The Hanover Insurance Company
440 Lincoln Street, Worcester, MA 01653

hanover.com
The Agency Place (TAP)—https://tap.hanover.com

119-0475 (5/16) LC 2015-399