LAWYERS MUTUAL

Scam Alert
Fake Wiring Instructions

If you are holding funds in trust for disbursement and receive a change in payment instructions, STOP.

Changes in wiring instructions may not be legitimate.

Scammers have infiltrated the email accounts of realtors to send altered wiring instructions - but the same scammers could also infiltrate the emails of clients, other services providers, and even law firms in order to steal client funds.

See the following alert from Peter Bolac of the North Carolina State Bar.:

> To: All Members of the North Carolina State Bar
> From: Peter Bolac, Trust Account Compliance Counsel
>
> Last week, the Bar received multiple reports of fradulent activity relating to wired funds in real estate transactions, with losses as high as $200,000. Here is a redacted sample of what we have received:
>
> "On a closing that took place on Friday morning, before we disbursed, we received an email and a phone call from a lady purporting to be our out of state seller asking us to wire funds to her bank account. On Monday we learned that the seller's email was compromised and bad actors had inserted themselves in her place. We attempted to retract the wire and we learned late yesterday that the bank did not retract the wire and will not communicate further without a subpoena."
>
> This firm had two-level confirmation practices in place to protect against fraudulent wires, but the hackers emailed and called the firm to confirm the wiring instructions as was required. The hackers gained access to the email account of one of the parties to the transaction and learned the necessary information in order to assume the identity of one of the parties and initiate the fraudulent transaction. Another defrauded firm noticed after the fact that the email address of the hacker was different from the actual seller's email address by one letter.
>
> One way to protect against this fraud is for the lawyer to initiate the phone call to confirm the emailed wiring instructions, calling only the number in the client file even if a different number is provided via email. Please be vigilant when communicating over email and consider whether your firm's wiring procedures are strong enough to detect and prevent these fraud attempts. If your firm has been the subject of an attempted or successful fraud, please contact me at the State Bar at pbolac@ncbar.gov or (919) 828-4620.
>
> Peter Bolac
> Trust Account Compliance Counsel
> North Carolina State Bar

Call Lawyers Mutual to report possible fraud or cybercrime.

Frauds and Scams that Target Lawyer Trust Accounts

by Peter Bolac, NC State Bar

Peter Bolac is Trust Account Compliance Counsel and District Bar Liason for the NC State Bar. Contact Peter at 919-828-4620, or email pbolac@ncbar.gov.

The State Bar continues to receive reports of frauds and scams on lawyer trust accounts resulting in six-figure losses. The three major types of scams are 1) Email initiated counterfeit bank checks 2) Forged trust account checks, and 3) Compromised wire instructions. The following is a brief summary of each scam.

Counterfeit Check Scam

By now, all lawyers should know that criminals are using email to act like potential clients requesting representation (typically commercial debt collection or divorce settlement collection). Once the lawyer responds with a request for more information, the "client" provides the lawyer with documentation of the "debt", often including warehouse receipts, contracts, bills of lading, etc. Shortly after agreeing to pursue the claim and often before a demand letter is even drafted, the lawyer receives a letter and certified bank check from the supposed debtor who is paying because they "don't want to deal with the law." The lawyer then deposits the certified bank check (often from a bank up north like Chase so the tellers are less familiar with it) into the trust account. Almost immediately, the client begins demanding his payment via wire. Since the funds are available via provisional credit, the lawyer wires out the money to the client minus the lawyer's share. The client is never heard from again. Three days later, the bank tells the lawyer that the check was counterfeit and removes the already wired amount from the trust account. Since the lawyer disbursed on provisional credit, the lawyer is responsible for replenishing any trust account deficit. This type of scam has cost lawyers hundreds of thousands of dollars and at least one law license. For tips on detecting and avoiding this scam, view this fact sheet created by Canadian indemnity company, LawPro: http://practicepro.ca/practice/pdf/FraudInfoSheet.pdf

Forged Trust Account Checks

The Bar is receiving an increased number of reported thefts via forged trust account checks. In this scenario, a criminal obtains the lawyer's account information (account number/routing number) and creates a fake check payable to cash. The criminal then negotiates that check at a check cashing company with a forged signature. While the lawyer may have recourse to recover the stolen funds from the bank if it honored the checks, in the interim the lawyer has to deal with a shortage in the trust account and outstanding checks that may bounce. The lawyer may also need to open a new trust account since the old account was compromised. One way to prevent this potential scenario is to enroll in a bank's positive pay program so only law firm approved checks are honored. Lawyers should review their trust accounts regularly to look for unapproved or unidentified transactions.

Compromised Wire Instructions

The most recent and most alarming type of scam is one where the criminal gains access to the email account of a party to a real estate transaction and initiates a fraudulent wire transfer. Once an account has been hacked, the criminal learns the details of the real estate transaction and, acting like the seller, emails the lawyer with wiring instructions for the seller's funds. Even law firms with two-level confirmation procedures for wire instructions have been defrauded because the criminal calls the firm as the seller and confirms the wiring instructions. The firm wires the money to the criminal's account and it is never seen again. Further, the bank denies any liability because it merely followed the lawyer's instructions. This scheme has caused hundreds of thousands of dollars of losses in the last week alone. One firm noticed after the fact that the email sent from the "seller" was one letter different than the real seller's actual email address. To prevent this type of theft, law firms should initiate the phone call to confirm the emailed wire instructions, calling only the number listed in the client file regardless of whether a different number is provided in the email.

While these three types of scams vary in sophistication, all three have the potential to cause significant harm and lawyers must remain vigilant for any fraudulent trust account activity. If you or your firm has been subject to any attempted scams, or if you have any questions regarding these scams, please contact me.

Real Estate Attorneys Take Note: Funds Transfer Fraud or Social Engineering Fraud?

by Adam Pierce, Lawyers Insurance

Adam Pierce, AAI, is the Director of P&C Operations at Lawyers Insurance. Contact Adam at 919-677-8900, or email adam@lawyersmutualnc.com.

Funds Transfer Fraud coverage is available on most crime insurance policies, and is one we highly recommend. Most firms are concerned about someone initiating a fraudulent transfer on their behalf. However, there is a relatively new phenomenon we are seeing – social engineering fraud. This is the deceptive gain of an employee's trust to induce him or her to part with money or securities.

Here is an example of social engineering fraud. Your firm is handling a closing for a residential real estate client. Right before closing, you get an email from the realtor providing you new wiring instructions for the funds. You work with this realtor often, and don't think to question this request. You wire the funds only to later find out that the realtor's email was hacked, and the money is gone.

Would standard Funds Transfer Fraud coverage cover this event? No, for Funds Transfer Fraud coverage to apply, the instruction must have appeared to come from the insured firm. In this case, the firm actually sent these instructions to the bank, so coverage would not apply. If a hacker had sent them to the bank, coverage would apply.

Enter Social Engineering Fraud Coverage. This relatively new product is designed to cover situations in which deception is used to induce your firm to voluntarily part with money. Anyone handling large sums of money, such as real estate attorneys, should consider this coverage. Only a few carriers provide this coverage, and the additional coverage increases the price somewhat, but also provides much greater protection.