



Primer On Avoiding Wire Fraud

Background

A major risk that real estate professionals should be aware of is fraudulent Wiring Instructions. Cyber-criminals are increasingly sending false messages on behalf of home sellers, home buyers or borrowers, real estate brokers, title companies, and lenders, regarding the transfer of funds associated with a real estate transaction.

Email hacking is a primary tool utilized by cyber-criminals. In many instances, the criminals create alternative email accounts applying minor changes to the name of the email account. Those changes typically go unnoticed by the recipient of the now fake email. How do these scams work?

Often hackers monitor email exchanges between the parties of a real estate transaction and gain specific information, such as the buyer and seller names, property address, and associated file numbers. As a closing date approaches and arrangements are made to wire money to a settlement agent or wire the proceeds from the sale of the house to the sellers, the scammer will send a last-minute email from a hijacked account or similar looking email address “revising” the Wiring Instructions. This “update” to the prior Wiring Instructions could result in the funds being transferred into a fraudulent bank account instead. On its face, the fraudulent email looks legitimate and often displays transaction specific information in the body of the email or in an attachment the hackers obtained through illegal means.

“Unfortunately the costs to Colorado consumers can be in the tens to hundreds of thousands of dollars with just one successful scam,” stated Marcia Waters, Director of the Colorado Division of Real Estate. “Unless you pay very close attention, everything may look right -- the email signature, address and the website. But, by the time homebuyers realize something is wrong, the money is already gone and in an untraceable bank account, leaving them at the closing table with no money and eliminating their ability to purchase the home.” This past February, a Colorado seller lost over \$80,000 from the sale of their property to one of these scams!

Precautionary Procedures

Here are some precautionary measures you should consider from a risk management perspective to reduce the chances of falling victim to fraudulent Wiring Instructions:

Be Mindful of Links and Attachments. Cyber criminals use attachments and links to gain access to emails and other login credentials, along with your other personal information. Beware of phishing emails embedded with links and attachments from unknown addresses.

Review Emails and Verify Instructions. If Wire Instructions are received via email, mail or phone, you should always verify you are speaking with the right party by meeting in person or utilizing a call back procedure using a phone number from a third-party (independent) source. This call back practice will ensure you are confirming with the correct individual and proper information. If Wiring Instructions are ever changed, you should presume the change to be fraudulent (better to act with caution than



without). Review the modified instructions in detail for any inconsistencies and always follow a call back procedure for independent verification purposes.

Communicate With Your Team and Clients. Precautions serve no purpose if the necessary people aren't informed. Communicate to your employees, clients, and business partners about this industry threat. The reason for any such protocols is to safeguard client funds.

Keep a record of websites that hold your financial information. Before providing financial information to others, confirm that the websites in which you input and retrieve your financial information are secure. Look for URLs that start with HTTPS, the "S" stands for secure.

Update your computer. Always keep your operating system, browser and security software up-to-date. Make sure that your email is protected. Change your password regularly and do not use "simple" passwords.

Some Red Flags Specific To Wire Fraud

- ✓ Using unsecure email to change Wiring Instructions – always confirm by calling a verified and known phone number and presume the email is fraudulent.
- ✓ Persistent emails - multiple emails being sent minutes apart – trying to create a sense of urgency for last minute changes regarding a real estate closing.
- ✓ Refusing to discuss by phone - criminals sending fraudulent emails will refuse to discuss last minute changes by phone (they make an excuse that they are in meetings and unable to call)
- ✓ Poor grammar and incorrect spelling - may help identify a fraudulent email.
- ✓ Repeated requests to keep the transaction confidential - whenever wire transfer instructions specify to keep the transaction "secret", you should verify the legitimacy of the source of the request. Speak to the executive or manager requesting the transaction be secret by phone or in person. If you still have doubts, ask to speak to another, more senior executive.
- ✓ Suspicious looking email addresses or domains - double and triple-check email addresses. Instead of (or in addition to) hacking an account, a common trick is to masquerade as a party to the transaction by modifying an email address slightly so an employee doesn't notice that the message is from a fraudulent domain. By replacing the "w" in Bank of the West's name with a double "v," for example, a masquerader was able to send emails from Bankofthevest.com. Replacing an "L" with an "I" or a "1" in ColdwellBanker.com is another example.
- ✓ Suspicious patterns - fake Realtor™ calls to request information and then exploiting emails with revised Wiring Instructions for transmitting seller's proceeds or other funds to a bogus bank account. For brokers, review your sent emails to cross-reference replies that you did not send.
- ✓ The New Deal out of Nowhere – be leery of email contact only out-of-the-blue with a new contract and associated check for earnest money. Expect an immediate request to return all or a portion of the earnest money via wire transfer for the funds delivered via the check. The check is likely fraudulent and you are now wiring funds to an untraceable bank account.
- ✓ Slow down - speed is the fraudster's ally and your enemy. Fraudsters gain an advantage by pressuring people to take action quickly without independent confirmation of all the facts. Be on high alert for possible fraud anytime wire transfer instructions include tight deadlines or last minute changes revolving around a pending real estate transaction.



A Broker Contract Disclaimer

This is an example of a Disclosure that could be used by a Broker for contract management purposes:

WIRE FRAUD DISCLOSURE

Criminals are targeting email accounts of various parties involved in a real estate transaction (e.g., lawyers, title companies, mortgage brokers, and real estate brokers). Fraudulent wiring instructions are being used to divert funds to the criminal's bank account. These emails may look like legitimate emails from a party to your transaction. Broker strongly recommends that you, your attorneys, and all others working on a transaction, should refrain from transmitting any non-public personal and financial information in an email, directly in the body of the email or through an email attachment. If you need to transmit social security numbers, bank accounts, credit card numbers, wiring instructions or similar private information, Broker strongly recommends that you utilize a secure method, such as providing the information in person, over the phone, or through secure mail. In addition, before you wire any funds to any party (including your lawyer, title company, mortgage broker, or real estate broker) call that party first to confirm the instructions are legitimate and correct.

Before any contemplated funds are sent, advise your clients to verify wiring instructions over the phone with the title company. This includes verbal verification of all escrow account information with the title company, not just that the Wiring Instructions were sent.

What We Are Doing

- Title Company of the Rockies will only send you our Wiring Instructions via our encrypted email technology.
- If you receive an email containing new or revised Wire Transfer Instructions, immediately call your escrow officer to verify the information prior to sending funds or other information. Again, we will always send you our Wiring Instructions directly, and only through encrypted email.
- You can send us your information via our encrypted email technology. You can initiate that process by using the button provided in our email signature blocks and also available on the home page of our website, www.titlecorockies.com or <https://securemail-titlecorockies.com>.
- Title Company of the Rockies will **not** accept your Wiring Instructions via email. Contact your Escrow Officer for the details on how we will receive and accept your Wiring Instructions. We will always independently verify your Wiring Instructions directly with you.
- We cannot process incomplete or inaccurate Wiring Instructions. You should verify that the routing number, account number, and the name applicable to the account are correct before submitting any wire transfer instructions to us.
- International wires will receive extra scrutiny. We will only wire funds out directly to the parties (as account holders) to a transaction and never to delegated parties.
- Title Company of the Rockies maintains a Cyber-Liability Insurance Policy on behalf of our customers.

The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) recently issued an Advisory intended to help identify and prevent email wire fraud schemes directed at financial institutions and their customers. The Advisory can be found at <http://image.exct.net/lib/fef91775716d05/m/1/FinCEN+Advisory+FIN-2016-A003.pdf>. Any fraudulent activity should be reported to the Federal Bureau of Investigations through its Internet Crime Complaint Center at <https://www.ic3.gov>.

This Primer is being provided for general information purposes only. Seek independent legal or tax advice for any specific transaction or individual questions you might have. Some source material can be attributed to our title insurance underwriters, Land Title Association of Colorado, and the Colorado Division of Real Estate. © 2017