TitleNews Online Archive

Colorado Warns of Fraudulent Wire Scams

December 15, 2016

The Colorado Division of Real Estate at the Department of Regulatory Agencies (DORA) issued a warning issued a warning to consumers about email and money wiring scams.

DORA reported that it continues to receive information about the scam in which cybercriminals hack the email accounts of real estate brokers, title companies, and consumers who are in the process of buying or selling a home. In other instances, they create alternative email accounts with just minor changes to the name of the email account, which typically goes unnoticed by the recipient of the email.

The Federal Trade Commission and Financial Crimes Enforcement Network (FinCEN) issued similar warnings to guard against the growing number of email fraud schemes involving wire transfers.

How do the scams work? Often the computer hackers monitor email exchanges between the parties of a real estate transaction and gain specific information, such as the buyer and seller names, subject property address and file numbers. As the closing date approaches and arrangements are made to wire the money to the closing company, 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 updating the wiring instructions to request the money be transferred into a fraudulent bank account. The email looks legitimate and often contains the transaction specific information the hackers obtained in the body of the email or as an attachment.

“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 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.

Title and settlement companies can protect themselves by increasing staff awareness of these scams. According to the FBI, businesses that deploy robust internal prevention techniques at all levels (especially targeting front line employees who may be the recipients of initial phishing attempts), have proven highly successful in recognizing and deflecting email scam attempts. Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of the request. ALTA's **Title Insurance and Settlement Company Best Practices** details policies and procedures title and settlement companies should follow to protect money and non-public personal information.

Red Flags

- A customer's seemingly legitimate emailed transaction instructions contain different language, timing, and amounts than previously verified and authentic transaction instructions.
- Transaction instructions originate from an email account closely resembling a known customer's email account; however, the email address has been slightly altered by adding, changing, or deleting one or more characters. For example:

Legitimate email address

  - john-doe@abc.com

Fraudulent email addresses

  - john_doe@abc.com
  - john-doe@bcd.com

- Emailed transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used.
- Emailed transaction instructions direct wire transfers to a foreign bank account that has been documented in customer complaints as the destination of fraudulent transactions.
- Emailed transaction instructions direct payment to a beneficiary with which the customer has no payment history or documented business relationship, and the payment is in an amount similar to or in excess of payments sent to beneficiaries whom the customer has historically paid.
- Emailed transaction instructions include markings, assertions, or language designating the transaction request as "Urgent," "Secret," or "Confidential."
- Emailed transaction instructions are delivered in a way that would give the financial institution limited time or opportunity to confirm the authenticity of the requested transaction.
- Emailed transaction instructions originate from a customer's employee who is a newly authorized person on the account or is an authorized person who has not previously sent wire transfer instructions.
- A customer's employee or representative emails a financial institution transaction instructions on behalf of the customer that are based exclusively on email communications originating from executives, attorneys, or their designees. However, the customer's employee or representative indicates he/she has been unable to verify the transactions with such executives, attorneys, or designees.

- A customer emails transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful.
- A wire transfer is received for credit into an account, however, the wire transfer names a beneficiary that is not the account holder of record. This may reflect instances where a victim unwittingly sends wire transfers to a new account number, provided by a criminal impersonating a known supplier/vendor, while thinking the new account belongs to the known supplier/vendor, as described in the above BEC Scenario 3. This red flag may be seen by financial institutions *receiving* wire transfers sent by another financial institution as the result of email-compromise fraud.

Click here to learn more about phishing.