PashmanStein WalderHayden
A Professional Corporation

Beware of New Wire Transfer Dangers in Real Estate Transactions

Dec 11, 2014

RELATED ATTORNEYS

Bruce J. Ackerman

RELATED PRACTICE AREAS

Commercial Real Estate

I attended a real estate closing recently for a cooperative development and had a shocking story told to everyone by the buyer. The buyer had her gmail account hacked by someone overseas, and they sent emails that resembled her attorney's account. The email actually had a slightly different email address that included the firm name of her attorneys, and had the look and feel of the real emails she had previously received from them. They copied her attorney's firm logo as well. The final act was the email to her to wire transfer her closing funds to an account in Miami, Florida. All the details required for the wire were included, even the phone number to verify the information.

The buyer initiated the wire of funds that was required for the closing later that day. The buyer did not realize that the trust account of her NJ attorney had to be in a NJ bank. Only due to her bank calling the attorney's office was the hacking revealed, saving this buyer from a mistake of more than $500,000. She also called the number on the wire sheet, and someone answered, but obviously not from the attorney's office.

In this transaction, the hackers did not stop, still falsifying emails to the buyer's attorney. The personnel at the attorney's office eventually wired out funds intended for the sellers, but wired the money to the hackers based upon another fake email with wire instructions.

This is a new hacking method being reported in real estate related transactions. The fraud targets wire transfers in real estate transactions, including wires of earnest money deposits and, as shown, closing proceeds. Apparently, these criminals hack into and intercept emails by searching for wire transfer requests and the emailing of the 13 digit number that makes up the digits in bank accounts. The hackers then start their process of "invading" the communications and intercept the lawful ones. The fake emails have the same attributes as the real ones

they are meant to resemble. They may keep communicating with the target victim, so that there is no suspicion that a third party has hacked into the stream of emails.

The hackers may even use the same bank and just change the last numbers for the account to be credited. If the funds get wired, the money will be gone and wired out overseas before the fraud is even noticed.

In order to ensure the safety of wire transfers, far more caution is needed. Here are a few precautions to be taken, including one very simple one. If you are sending a wire, you should contact the party who sent the instructions by phone to confirm the account numbers verbally prior to sending the funds. Another precaution is to send wire instructions via encrypted email or fax only. Beware.