WIRE FRAUD
PREVENTION TIPS

Wire fraud has become a daily occurrence in our industry. Realtors®, Real Estate Brokers, Buyers and Sellers are targets for wire fraud and many have lost hundreds of thousands of dollars because they wired funds based on wire instructions received via email.

Common Wire Fraud Schemes

A hacker can break into a licensee's email account to obtain information about upcoming real estate transactions. After monitoring the account to determine the likely timing of a close, the hacker sends an email to the buyer, posing either as the escrow agent or as the licensee.

The fraudulent email may contain new wiring instructions or routing information, and request that the Buyer send funds accordingly. They could just as easily send an e-mail to the escrow agent posing as a Seller or a Real Estate Broker instructing the escrow agent to wire seller funds to different account rather than to the account provided at the signing.

Be Alert

Below are the procedures we have implemented at Ticor Title to keep our clients' information and money safe and secure. We have also provided some tips on what a client should look for.

We encourage you to pass them along to your client so they are aware of the wire fraud scams plaguing our industry.

1. Ticor Title will not accept disbursement instructions or changes to disbursement instructions via e-mail. Should a circumstance arise that requires disbursement instructions be sent via e-mail we will always contact the client to confirm the information received using a pre-verified phone number.
2. If we are instructed to e-mail wire instructions to a Broker or a Buyer or Seller they are always sent using encrypted e-mail.
3. If your client receives wire instructions via e-mail instruct them to ALWAYS follow up with a phone call to their escrow closer before they wire funds.
4. Pay attention to the wording of an email requesting funds. Many fraudsters are "offshore" offenders and their sentence structure may be broken and may contain misspelled words or improper grammar.
5. Beware of e-mail spoofing. E-mail spoofing is the forgery of an e-mail address so that the message appears to have originated from someone other than the actual source. For instance, you could receive an e-mail that you believe originated from your Escrow Closer or Broker because the e-mail address is the same as theirs. However, if you click on the e-mail address it will disclose the true e-mail address of the originator. E-mail Spoofing is a common tactic used in wire fraud campaigns and if you are not familiar with the tactic you are very likely to follow the instructions contained in the e-mail, believing they came from the proper party.
6. Be wary of a sudden or urgent request for funds that were not anticipated or required as part of the transaction. Examples include a request for an additional earnest money deposit or extension fee that was not part of the purchase agreement.

ALWAYS CALL BEFORE YOU WIRE.

When in doubt, always call our office or your escrow officer.

TICOR TITLE™