

# Fraud Alert!

We would like to alert you to a fraud scheme that could result in the theft of money from you or your customers. Here is how the scheme works:

1. The fraudster hacks into the e-mail accounts of a person related to real estate transactions (e.g. real estate agent or mortgage broker) without their knowledge.
2. The fraudster monitors e-mails to find details of upcoming closings.
3. The fraudster learns the parties' names, the amount of the deposit, the entity holding the deposit and other details.
4. The fraudster sends an e-mail to the buyer from the real estate agent's, mortgage broker's, or escrow agent's e-mail address. The e-mail looks normal in every way. The email may also include legitimate attachments that match the documents in real estate agent's file or the escrow file.
5. The fraudster's e-mail directs the buyer or escrow officer to wire the funds to a bank account other than that shown in the preliminary report or commitment, escrow instructions, or commission demand. In reality, the wire instructions are to an account controlled by the fraudster.
6. If the money is wired as instructed, it is gone for good, and has been stolen from the buyer, seller, or escrow account by fraud.

Don't let this happen to you!

1. Verify any e-mails providing wire instructions for disbursement of funds from the escrow by phone using known legitimate phone numbers. Don't use the phone number in the email received for the disbursement of funds.
2. All parties are encouraged to contact your escrow agent immediately if the wiring instructions for deposit of funds with your escrow agent request the funds go to a bank branch or account outside your state.
3. Inform all parties to the transaction (buyers, sellers, real estate agents and lenders) about this scheme and ask them to be on the lookout for responses to e-mails they have not sent. This may be a sign that their e-mail account has been hacked.