WIRE SAFE™ | Inquire before you wire!

February 28, 2018

Wire Fraud Alert!

This Notice is not intended to provide legal or professional advise. If you have any questions, please consult with a lawyer.

Realtors®, Real Estate Brokers, Closing Attorneys, Buyers and Sellers are targets for wire fraud and many have lost hundreds of thousands of dollars because they simply relied on the wire instructions received via email, without further verification. A fraudster will hack into a participant's email account to obtain information about upcoming real estate transactions. After monitoring the account to determine the likely timing of a closing, the fraudster will send an email to the Buyer purporting to be the escrow agent or another party to the transaction. The fraudulent email will contain new wiring instructions or routing information, and will request that the Buyer send funds to a fraudulent account.

PLEASE BE ADVISED THAT WE ONLY PROVIDE WIRING INSTRUCTIONS THROUGH VERBAL COMMUNCATION. If funds are to be wired to us in conjunction with the transaction and/or you receive another email or unsolicited call purporting to provide you with wiring instructions, please give us a call immediately.

In addition, the following non-exclusive self-protection strategies are recommended to minimize exposure to possible wire fraud:

1. **NEVER RELY** on emails purporting to change wire instructions. Parties to a transaction rarely change wire instructions in the course of a transaction.
2. **ALWAYS VERIFY** wire instructions, specifically the ABA routing number and account number, by calling the party who sent the instructions to you. DO NOT use the phone number provided in the email containing the instructions, use phone numbers you have called before or can otherwise verify. **Obtain the number of your Realtor®, Real Estate Broker and your escrow officer as soon as an escrow account is opened.** DO NOT send an email to verify as the email address may be incorrect or the email may be intercepted by the fraudster.
3. **DO NOT** forward wire instructions to other parties without first verbally verifying the instructions from the sending party.
4. **USE COMPLEX EMAIL PASSWORDS** that employ a combination of mixed case, numbers, and symbols. Make your passwords greater than eight (8) characters. Also, change your password often and do NOT reuse the same password for other online accounts.
5. **USE MULTI-FACTOR AUTHENTICATION** for email accounts. Your email provider or IT staff may have specific instructions on how to implement this feature.

For more information on wire-fraud scams or to report an incident, please refer to the following links:

Federal Bureau of Investigation: http://www.fbi.gov ***Internet Crime Complaint Center:*** http://www.ic3.gov