WIRE FRAUD ADVISORY

The ability to communicate and conduct business electronically is a convenience and reality in nearly all parts of our lives. At the same time, it has provided hackers and scammers new opportunities for their criminal activity. Many businesses have been victimized and the real estate business is no exception.

While wiring funds is a welcome convenience, buyers and sellers need to exercise extreme caution. Emails attempting to induce fraudulent wire transfers have been received and have appeared to be legitimate. Reports indicate that some hackers have been able to intercept emailed wire transfer instructions, obtain account information and, by altering some of the data, redirect the funds to a different account. It also appears that some hackers were able to provide false phone numbers for verifying the wiring instructions. In those cases, the buyers called the number provided, to confirm the instructions, and then unwittingly authorized a transfer to somewhere other than escrow. Sellers have also had their sales proceeds taken through similar schemes.

ACCORDINGLY, BUYERS AND SELLERS ARE ADVISED:

1. Obtain the phone number of the Escrow Officer at the beginning of the transaction. DO NOT USE ANY OTHER TELEPHONE NUMBER TO CONTACT YOUR ESCROW OFFICER.

2. DO NOT EVER WIRE FUNDS PRIOR TO CALLING YOUR ESCROW OFFICER TO CONFIRM WIRE INSTRUCTIONS. ONLY USE A PHONE NUMBER YOU WERE PROVIDED PREVIOUSLY.

3. Verbally confirm the wire transfer instruction is legitimate and confirm the bank routing number, account numbers and other codes before taking steps to transfer the funds.

4. Avoid sending personal information in emails or texts. Provide such information in person or over the telephone directly to the Escrow Officer.

5. Take steps to secure the system you are using with your email account. These steps include creating strong passwords, using secure Wi-Fi, and not using free services.

If you believe you have received questionable or suspicious wire instructions, immediately notify your bank, the Escrow Holder and your real estate agent.

RED FLAGS

Following, are some red flags to watch for when receiving communication regarding your transaction:

- Messages that appear to be from your escrow officer that comes from a “free” email account, such as gmail, yahoo, and other non-secure email addresses. Your escrow officer will NEVER send you an email from one of these accounts. Our company uses only SECURE HOSTED EMAIL SERVICES.

- Wire instructions that list the beneficiary (receiving party) as anyone other than our company. Your escrow officer will only provide you with wire instructions that direct your funds to an escrow or title trust account in the name of our company.

- Emails or other communication that provides you with a telephone number, physical address or email address that does not match our initial communication with you.

- A sudden sense of urgency in an emailed request for you to wire your funds. ALWAYS contact your escrow officer using the telephone number given to you at the start of your transaction to verify wire instructions. DO NOT rush to send a wire before you speak with your escrow officer.

Your escrow officer may send sensitive information, such as wire instructions, using encrypted email services. These services may require you to create an account to read and reply to the message. Please be patient and understand that our goal is to protect you, your personal information and your funds.

Your escrow officer may also provide you with a personal password at the beginning of your transaction as an additional security measure. Please keep your password secure and handy to provide to your escrow officer when communicating by telephone. Your escrow officer will NEVER ask you to email, fax or mail this password.

By signing below, the undersigned acknowledge that each has read, understands and has received a copy of this Wire Fraud Advisory.