BUYER/SELLER CYBER PROTECTION NOTICE

Housing transactions of any type will require you to submit personal information to a lender, title company and/or settlement or escrow agent. This information may include Social Security numbers, bank account numbers, credit and loan account information. While those involved in your transaction are working on your behalf, other would-be criminals may sometimes attempt to access your personal information and may even try to access money through real estate transactions.

Watch for these 4 Cyber Fraud Red Flags

Email messages that are not official

- Always carefully examine the email address that you receive that contains updates on your transaction from your real estate agent, escrow officer or settlement agent.

Receiving an email with NEW Wiring Instructions

- Call your escrow officer or settlement agent immediately
- If you receive wiring instructions, even if it appears legitimate, **do not send any money** to that account..
- Always contact the closer directly before any money is wired.
- Do not use a phone number or other contact information from an email you received.
- Use a business number from another source (such as the closing company's website) to make sure you are actually talking to your closer and not an imposter intent on stealing your money.

Receiving an inbound call from someone claiming to be working on your transaction

- Never give information about yourself or your transaction to any unknown party.
- Confirm any changes to the transaction with your real estate, escrow or settlement agents in person or over a phone call you make to them

Hacking into your email accounts

- If you suspect your email is being improperly used or if you do not receive funds in a timely manner, contact your settlement or real estate agent

I understand and acknowledge the above information:

_____ _____

BUYER/SELLER (circle one) BUYER/SELLER (circle one)