Wire Fraud Advisory Notice

File No.:

Address:

Date:

Cybercrime is a potential threat in real estate transactions because sensitive data, including social security numbers, bank account numbers, and wire instructions are often sent by electronic means. Instances have occurred where criminals have hacked email accounts of entities related to real estate transactions (such as lawyers, escrow holders, title company representatives, or real estate brokers and agents). Using email, hackers have invaded real estate transactions and used fraudulent wiring instructions to direct parties to wire funds to the criminals’ bank accounts, often to offshore accounts, with little chance of recovery. It also appears that some hackers have provided false phone numbers for verifying the wiring instructions. In those cases, the buyers called the number provided to confirm the instructions, and unwittingly authorized a transfer to somewhere other than the proper escrow account. Sellers also have had their sales proceeds taken through similar schemes.

PLEASE BE ADVISED THAT [INSERT AGENT’S FIRM NAME HERE] **WILL NEVER SEND VIA EMAIL WIRING INSTRUCTIONS RELATED TO YOUR TRANSACTION**. BUYERS ARE ALSO ADVISED:

1. You should obtain the phone number of the Closing Attorney at the beginning of the transaction.

2. NEVER WIRE FUNDS PRIOR TO CALLING YOUR CLOSING ATTORNEY TO CONFIRM WIRE INSTRUCTIONS EVEN IF THE COMMUNICATION APPEARS TO BE FROM A LEGITIMATE SOURCE. USE ONLY A PHONE NUMBER YOU WERE PROVIDED PREVIOUSLY. DO NOT use any different phone numbers included in an email that contains wire transfer instructions. It is imperative that this call be made to a number obtained in person from the individual or through other reliable means, NOT from a number provided in the email or the wiring instructions.

3. Orally confirm the wire transfer instructions are legitimate and carefully confirm the bank routing number and account number before taking steps to transfer the funds.

1. You should never send personal information, such as bank account numbers, social security numbers or other financial information, via email, text or other unsecured electronic communication. You should provide such information in person, over the telephone directly, or by secured electronic communication to the Closing Attorney’s Office.

5. Take steps to secure the system you are using with your email account. These steps include creating strong passwords and using secure Wi-Fi as well as two-step verification processes.

If an email or a telephone call seems suspicious refrain from taking any action until the communication has been independently verified. Promptly notify your bank, your real estate agent, and the Closing Attorney’s Office. The sources below, as well as others, can also provide information:

The Federal Bureau of Investigation: <https://www.fbi.gov/scams-and-safety>

The National White-Collar Crime Center: [WWW.NW3C.ORG](https://www.nw3c.org/)

On guard online: [WWW.ONGUARDONLINE.GOV](https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security)

The Internet Crime Complaint Center: [www.ic3.gov](http://www.ic3.gov)

I have read and understand the above advisory notice.

I have read and understand the above advisory notice.

Borrower/Buyer:

Borrower/Buyer: