



Parties to a real estate transaction need to exercise extreme caution when wiring funds in real estate transactions. Criminals/hackers target email accounts of real estate brokers and salespersons as well as other parties involved in real estate transactions, including mortgage brokers, closing attorneys, and title agents. In many cases, they have been able to intercept emailed wire transfer instructions, obtain account information and, by altering some of the data, use emails to redirect the funds to a different account. These emails are convincing and sophisticated and may look like legitimate emails from parties in the transaction.

In each real estate transaction, Parties are advised to:

- **Never wire funds without personally speaking with the intended recipient of the wire to confirm the routing number and account number.**
- **Verify that the contact information is legitimate. Recipients of wiring instructions should call using a phone number that is independently obtained and not use the number in an email.**
- **Never send personal information such as social security numbers, bank account numbers and credit card numbers, unless it is through secured/encrypted email or personal delivery to the intended recipient.**
- **Take steps to secure the system you are using with your email account such as using strong passwords and secure WiFi.**

If you believe you have received questionable or suspicious wire instructions, immediately notify your bank, the escrow agent, and your Realtor®.

By signing below, you acknowledge that you have read and understand and have received a copy of this Wire Fraud Advisory.

DATED

SIGNATURE

SIGNATURE

SAMPLE ONLY