

Buyers and sellers 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 every real estate transaction, Buyer and Seller 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 for the wire transfer recipient is legitimate. Buyer and seller should each call using a phone number that has been independently obtained, not the phone number contained in the email containing the wiring instructions.**
- **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 suspect that you have been victimized by wire fraud, immediately contact the Boston FBI field office at 857-386-2000 or file a complaint online at www.ic3.gov.**

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

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

DATED

SELLER / BUYER (*circle one*)

SELLER / BUYER (*circle one*)