CYBER / WIRE FRAUD ADVISORY

Buyers and sellers need to exercise extreme caution when wiring funds in real estate transactions. Criminals/hackers target email accounts of real estate licensees 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. You should look carefully at the entire email address as it may look legitimate but will contain some small change to fool you for example, joe@acme.com becomes joe@acrne.com a very hard distinction to pick up. If you believe you have received questionable or suspicious wire transfer instructions, immediately contact the title company/closing agent and your real estate professional.

Do NOT Initiate the Electronic Transfer of Funds (Wires) Without Double Checking the Legitimacy of the Destination

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 share personal information such as social security numbers, bank account numbers and credit card numbers, unless it is through secured/encrypted email or personal delivery (or phone call) 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 and email using a domain name account (safer than using a public account such as aol or gmail).**

If you suspect that you have been victimized by wire fraud:

1) Contact the financial institution immediately and ask them to do a "SWIFT recall".
2) Then call your local law enforcement immediately (town police department or county sheriff's office) to report the incident.
3) Then call the FBI immediately (24 hours or less) and let them know you are reporting the incident within 24 hours and file a complaint online at www.ic3.gov. Your chances of recovery are greater with less than 24-hour reporting.

To contact the FBI for Maine coverage:

Bangor: 207-947-6670 -- Portland: 207-541-0700 -- Boston, MA: 857-386-2000

Even if you cannot undo the damage, file a complaint as specified above as this will help track the criminals.

Again, Do Not Initiate Wires Without Double Checking the Legitimacy of the Destination