

BE CAUTIOUS: WIRE FRAUD AND CYBER CRIME

WHAT BUYERS AND SELLERS NEED TO KNOW

TIPS FOR WIRE FRAUD PREVENTION

- Do not open any suspicious emails, click on any links, or open any attachments; delete these emails
- Clean out your email account on a regular basis
- Antivirus and firewall software should be regularly monitored and updated
- Lock your screen or log out when you walk away from your device to prevent unauthorized access
- Use encrypted emails when sending confidential information
- Stay away from free/unsecured Wi-Fi (i.e., coffee shops, hotels, libraries, restaurants)
- Use strong passwords by making them unique and complex
- Shred any and all documents that contain personal information such as account numbers, driver's license number, social security number, credit card, debit card numbers, etc.
- Do not post transactional information on social media such as names and addresses as this information may be used by criminals

DO NOT TRUST EMAILS CONTAINING WIRE INSTRUCTIONS

If you receive an email containing wire transfer instructions, immediately call your escrow officer to ensure the validity of the instructions.

TRUST YOUR SOURCE OF INFORMATION

Never direct, accept or allow anyone in the transaction to consent to receiving transfer instructions without a direct personal telephone call to the individual allegedly providing the 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.

VERIFY AND NOTIFY

Before you wire funds to any party (including your lawyer, title agent, mortgage broker, or real estate agent) personally meet them or call a verified telephone number (not the telephone number in the email) to confirm before you act!

A NOTE TO AGENTS: *Inter Valley Escrow is committed to taking every precaution to protect our clients funds, and we need your help! Protect your clients by not using Yahoo, Hotmail, Gmail, AOL or other free easily-hacked email accounts. Encourage your clients to not email financial information, be cautious about opening attachments of files from emails, and keep their software up to date.*