WIRE FRAUD ADVISORY

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 wireless for work matters
- 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!

Immediately notify your banking institution and Settlement/Title Company if you are a victim of wire fraud.

COOK & JAMES

VICTIMS OF WIRE TRANSFER FRAUD MUST TAKE IMMEDIATE ACTION

01 Contact the financial institution wiring the funds with instructions to stop or rescind the transfer and place a freeze on remaining funds.

02 Contact your local FBI field office: GA (770) 216-3000. To lookup your local FBI field office, go to **https://www.fbi.gov/contact-us/field-offices**

03 File a complaint on the FBI's Internet Crime Complaint Center at **https://www.ic3.gov/default.aspx**

04 Notify all other parties to the transaction that may have been exposed to the attack. Real estate agents should contact their broker.

05 Change all usernames and passwords associated with any account that you believe could have been compromised.

ONLINE RESOURCES

There are many online sources that can provide useful information regarding similar topics including, but not limited to, the following sites:

The Federal Bureau of Investigations @ **https://www.fbi.gov/scams-and-safety**
The Internet Crime Complaint Center @ **www.ic3.gov**
The National White Collar Crime Center @ **http://www.nw3c.org/research**
On Guard Online @ **www.onguardonline.gov**