WIRE FRAUD ADVISORY

Criminals are targeting social media and email to steal information. This is particularly common in real estate transactions because sensitive data, including social security numbers, bank account numbers, and wire instructions are often sent by electronic means. We do not want you to be the next victim of wire fraud. Money wired to a fraudulent account is stolen money that typically cannot be recovered. Additionally, there is generally no insurance for this loss. You may never get the money back.

PROTECT YOURSELF

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.

DO NOT TRUST EMAILS SEEKING PERSONAL/FINANCIAL INFORMATION

- If you receive an email requesting personal/financial information or asking you to download, click on a link, send, and/or do anything that may seem unusual to you, call your escrow officer immediately prior to acting on the suspicious email to verify the validity of the email.

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.

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 Investigation @ 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

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.

The undersigned acknowledges receipt of this Wire Fraud Advisory.

Client	Date	Client	Date

VICTIMS OF WIRE TRANSFER FRAUD MUST TAKE IMMEDIATE ACTION

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

2. Contact your local FBI field office: AZ (623) 466-1999. To lookup your local FBI field office, go to https://www.fbi.gov/contact-us/field-offices.

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

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

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

ARIZONA REALTORS®

255 E. Osborn Rd., Suite 200 • Phoenix, AZ 85012
Phone: 602.248.7787 • Toll-free in AZ: 800.426.7274 • Fax: 602.351.2474
www.aaronline.com

Cyber Security and Wire Fraud Policies and Procedures

This document is for informational purposes only.
Brokers may choose to implement some or all of the below policies and procedures as they see fit for their brokerage.

BROKERS SHOULD USE THE BELOW INFORMATION ONLY AFTER HAVING CONSULTED INSURANCE AND LEGAL PROFESIONALS.

In order to protect yourself and your brokerage, the below provisions, which are not all-inclusive, are intended to assist Brokers in establishing office policies and procedures related to cyber security and wire fraud. These provisions are not a substitute for the retention of independent legal counsel. Brokers are strongly encouraged to seek the advice of an insurance professional regarding cyber fraud insurance coverage.

Overview

- Cyber security threats and wire fraud are on the rise. Criminals find creative ways to breach cyber security which could have negative results such as loss of monies, exposure of confidential information, identity theft, etc.
- The purpose of these policies is to outline the appropriate use of technology to safeguard business transaction files.

Cyber Security

1. Passwords
    a. Use strong passwords by making them unique and complex
    b. Regularly change passwords
    c. Do not use the same password for all accounts
2. Email Security
    a. Do not open any suspicious emails, click on any links, or open any attachments; delete these emails
    b. Clean out your email account on a regular basis
    c. Use encrypted emails when sending sensitive or confidential information
3. Wireless Use Security
    a. Use encrypted wireless for work matters
    b. Stay away from free / unsecured Wi-Fi (i.e., coffee shops, hotels, libraries, restaurants)
    c. Consider using a Virtual Private Network (VPN)
4. Use of Electronic Devices
    a. Lock your screen or log out when you walk away from your device to prevent unauthorized access
    b. Report stolen or lost devices
5. Software
    a. Antivirus and firewall software should be regularly monitored and updated
    b. Data should be backed up on several different platforms
6. Record Keeping/Disposal
    a. 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.
7. Social Media

a. Do not post transactional information on social media such as names and addresses as this information may be used by criminals

8. Other – Include any other items of importance

Wire Fraud

1. Client Discussions
    a. Discuss with your client your communication practices so the client knows what to expect and can exercise caution if contacted by a different means than previously discussed
    b. Provide a document to clients describing wire fraud risk
2. Transactional Wire Instructions
    a. Prior to wiring funds, advise your client to contact the intended recipient via a verified telephone number to confirm the wiring information is accurate
    b. Advise your client not to respond to any emails changing wire instructions by replying to that email or calling the number contained in the email
    c. Consider including in your email signature a warning about wire fraud
        - NAR suggests the following:

    IMPORTANT NOTICE: Never trust wiring instructions sent via email. Cyber criminals are hacking email accounts and sending emails with fake wiring instructions. These emails are convincing and sophisticated. Always independently confirm wiring instructions in person or via a telephone call to a trusted and verified phone number. Never wire money without double-checking that the wiring instructions are correct.

3. Evaluate communications
    a. Thoroughly review emails, texts and other forms of communications for typos and suspicious links
    b. Do not click on links
    c. Only call trusted phone numbers
4. Other – Include any other items of importance

Reporting Cyber Crime

- If you become aware of a breach of data or wire fraud, you should:
    - Contact the sender of the funds so that they can contact their bank to try to stop the funds from being delivered
    - Notify your broker immediately
    - Notify all affected parties so that they may take appropriate action
    - Change all of your passwords and usernames
- Following a breach, you as the broker may want to:
    - Talk to an attorney as there may be notification laws
    - Contact the police
    - Report the breach to the FBI Internet Crime Complaint Center at https://www.ic3.gov/default.aspx
    - Report the breach to your REALTOR® Associations